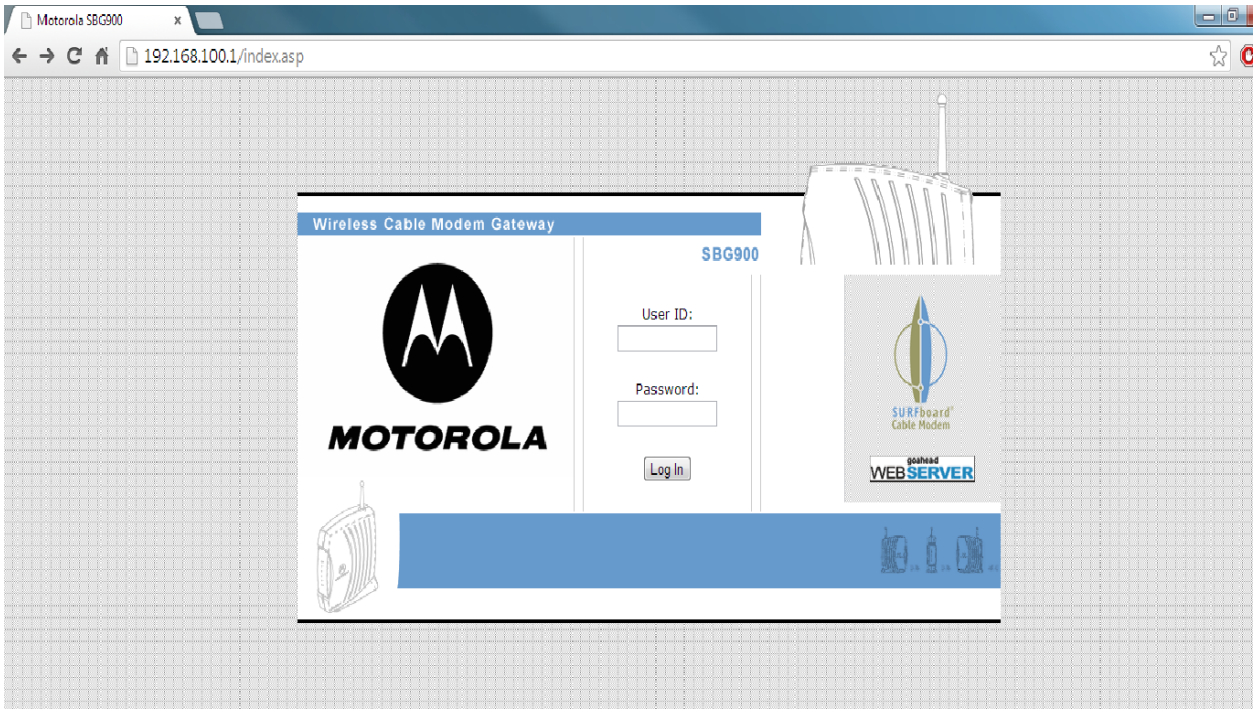
❖ Manual Motorola SBG900 Wireless Cable Modem Gateway

❖ Iniciando o Programa de Configuração do SBG900

1 Em um computador ligado ao SBG900 pela Ethernet ou USB, abra um navegador. Não tente configurar o SBG900 em uma conexão sem fio.

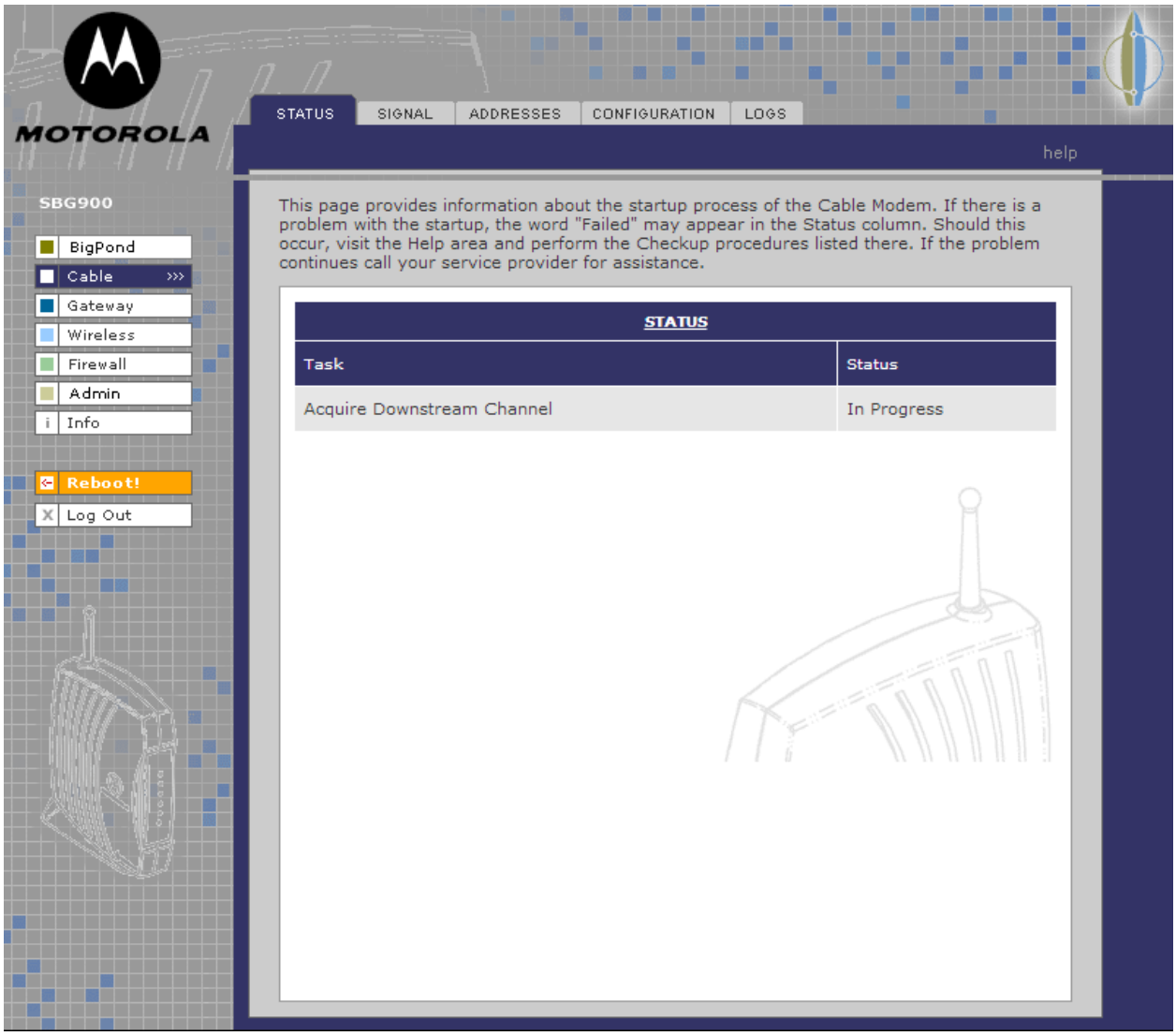
2 No campo de endereço, digite http://192.168.100.1 e aperte **ENTER** para aparecer a janela de Login:



3 No campo **User ID**, digite o usuário padrão “admin” (sem aspas).

4 No campo **Password**, digite a senha padrão “motorola” (sem aspas).

5 Clique em **Log In** para aparecer a janela de configuração e status do usuário do SBG900:



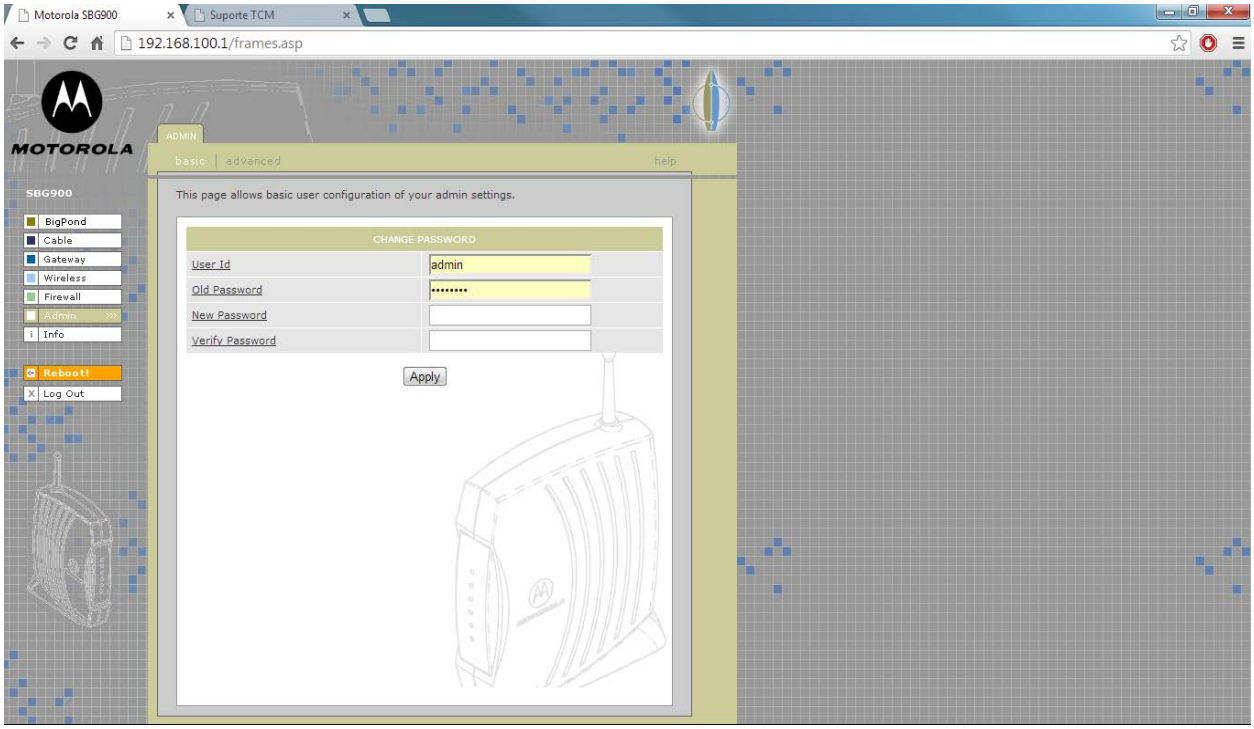
Cable Configurar e monitorar o sistema de conexão a cabo.
Gateway Configurar e monitorar as preferências do Gateway.
Wireless Configurar e monitorar a interface wireless.
Firewall Configurar e monitorar o firewall.
Admin Mudar a senha padrão.
Info Exibe informações sobre o programa de configuração do SBG900.
Reboot Reseta o SBG900. É a mesma coisa de apertar o botão de reset do painel traseiro por menos de cinco segundos.
Log Out Desloga do SBG900.

Observações: **Router** é uma opção de configuração que pode aparecer na sua janela, mas pode não ser suportada.

❖ Mudando a Senha Padrão

Para mudar a senha padrão:

1 Na tela do programa de configuração do SBG900, clique em **Admin** para exibir a página básica da guia.



2 No campo **Old Password,** digite a senha antiga. A senha padrão é “motorola” (sem aspas).

3 No campo **New Password,** digite a nova senha.

4 No campo **Verify Password,** digite a senha novamente.

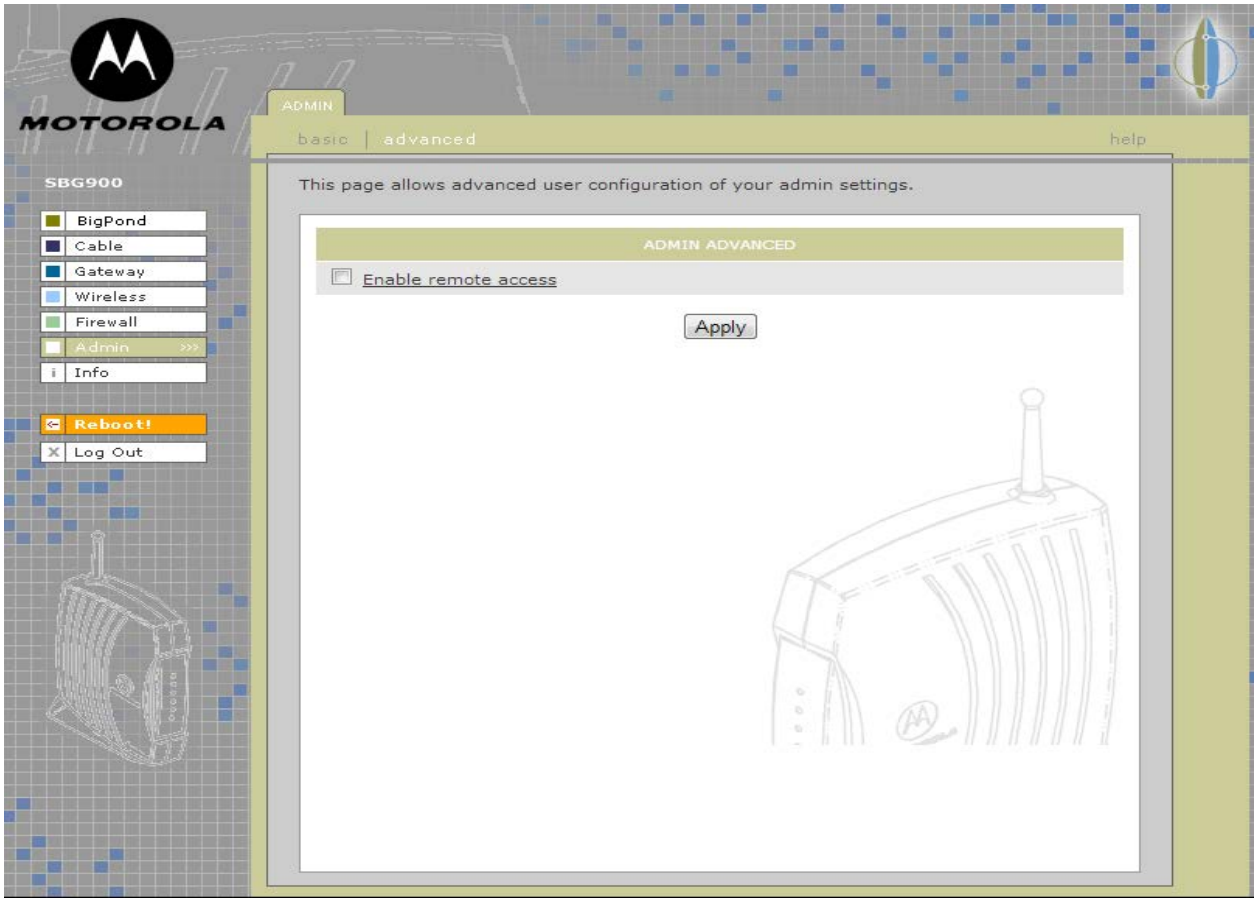
5 Clique em **Apply** para aplicar suas mudanças.

❖ Habilitando o Acesso Remoto

Habilitar o acesso remoto permite acessar o SBG900 através da Internet. Você deve conhecer a **User Id,** e o **Endereço IP público** designado para seu SBG900 para obter acesso às páginas de configuração através da internet. O acesso remoto é provido usando um Navegador Web no cliente remoto e conectando ao servidor Web no SBG900.

Para acessar o SBG900 remotamente:

1. Na tela do programa de configuração do SBG900, clique em **Admin** para exibir a página básica da guia.
2. Clique em **advanced** para mostrar a página avançada da guia.



3. Clique na caixa em frente a **Enable remote access** para habilitá-lo.
4. Clique em **Apply** para aplicar suas mudanças.

❖ Configurando um Hospedeiro DMZ

Alguns jogos e dispositivos de jogos requerem uma das duas coisas abaixo:

- O uso de portas aleatórias
- A exceção para passagem de tráfico não solicitado.

Por exemplo, para conectar um PlayStation 2 para jogar On-line, designe ele para ser um hospedeiro DMZ, pois as portas requeridas variam de jogo para jogo. Para estes jogos, nós recomendamos configurar o computador ou o dispositivo como o hospedeiro DMZ.

Para configurar um dispositivo de jogo DMZ, no Gateway > LAN – Página “dhcp leases”:

- Reservar um endereço de IP privado para o computador ou endereço MAC do dispositivo.
- Designar o dispositivo como um dispositivo DMZ.

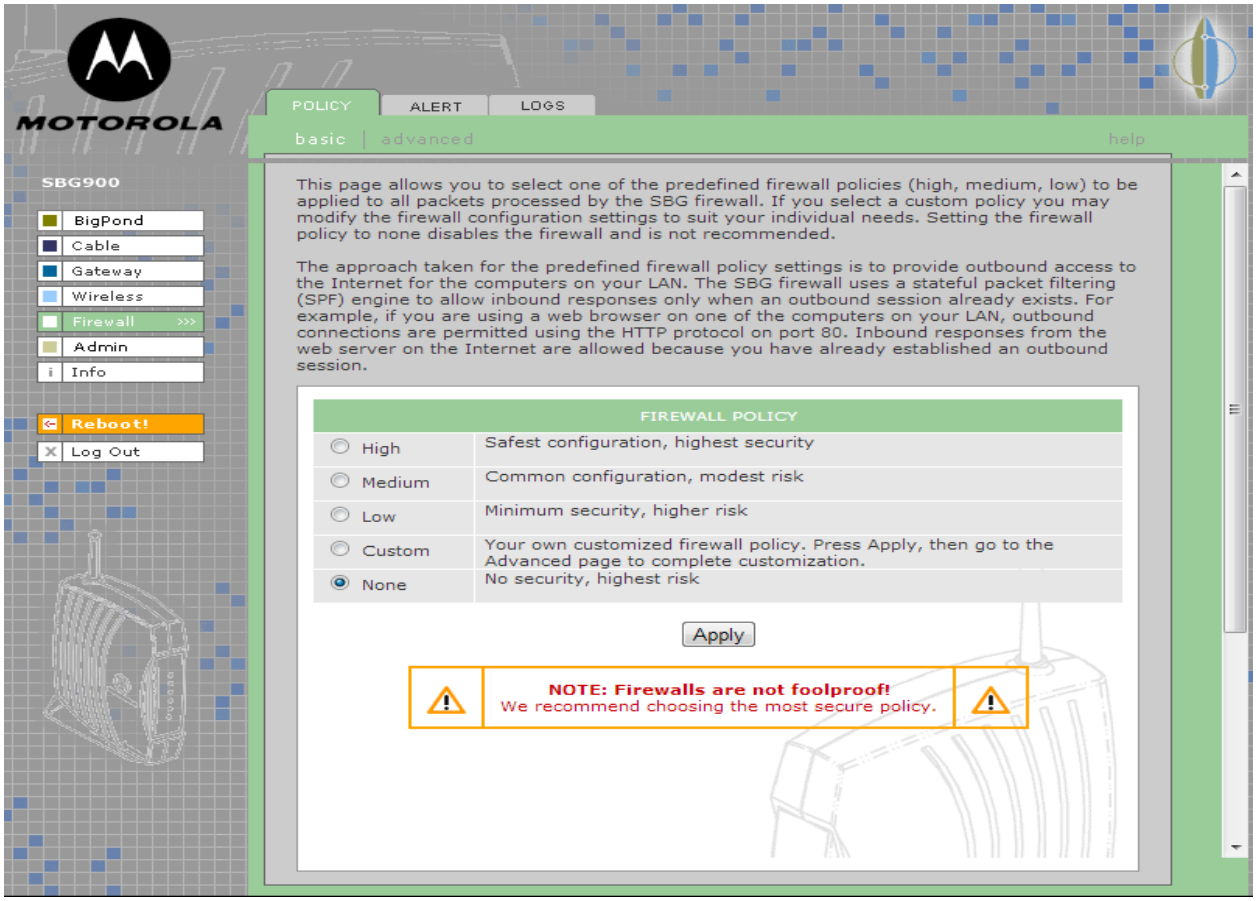
Você pode reservar endereços IP para múltiplos dispositivos, mas somente um pode ser designado como hospedeiro DMZ por vez.

❖ Configurando a Política do Firewall

O firewall do SBG900 protege a LAN do próprio de ataques indesejados e outras intrusões da Internet. Essa secção descreve o uso do Firewall > POLICY – página básica para escolher um dos modelos predefinidos de política do firewall fornecidos com o SBG900.

Para selecionar uma política predefinida para todos os pacotes processados pelo Firewall do SBG900:

1. No painel esquerdo do Programa de Configuração do SBG900, clique em **Firewall.**
2. Clique em **Policy.**
3. Clique em **basic** para exibir os modelos predefinidos de política de firewall.


MOTOROLA
POLICY
ALERT
LOGS
basic | advanced
help
SBG900
BigPond
Cable
Gateway
Wireless
Firewall
Admin
Info
Reboot!
Log Out
This page allows you to select one of the predefined firewall policies (high, medium, low) to be applied to all packets processed by the SBG firewall. If you select a custom policy you may modify the firewall configuration settings to suit your individual needs. Setting the firewall policy to none disables the firewall and is not recommended.
The approach taken for the predefined firewall policy settings is to provide outbound access to the Internet for the computers on your LAN. The SBG firewall uses a stateful packet filtering (SPF) engine to allow inbound responses only when an outbound session already exists. For example, if you are using a web browser on one of the computers on your LAN, outbound connections are permitted using the HTTP protocol on port 80. Inbound responses from the web server on the Internet are allowed because you have already established an outbound session.
FIREWALL POLICY
High
Safest configuration, highest security
Medium
Common configuration, modest risk
Low
Minimum security, higher risk
Custom
Your own customized firewall policy. Press Apply, then go to the Advanced page to complete customization.
None
No security, highest risk
Apply
NOTE: Firewalls are not foolproof!
We recommend choosing the most secure policy.

4 Selecione a política de firewall mais segura que você conseguir.

High:

O modelo de política de firewall predefinido mais que provê a maior segurança. A Motorola recomenda essa configuração.

Medium:

Um modelo de política de firewall predefinido que provê uma configuração comum, tendo um risco moderado.

Low:

Um modelo de política de firewall predefinido que provê mínima segurança, com um risco maior de intrusões.

Custom:

Você pode precisar criar uma política de firewall customizada indo até Firewall>POLICY – página avançada. Não crie uma política customizada a não ser que você tenha o conhecimento necessário, assim como uma necessidade de fazê-lo.

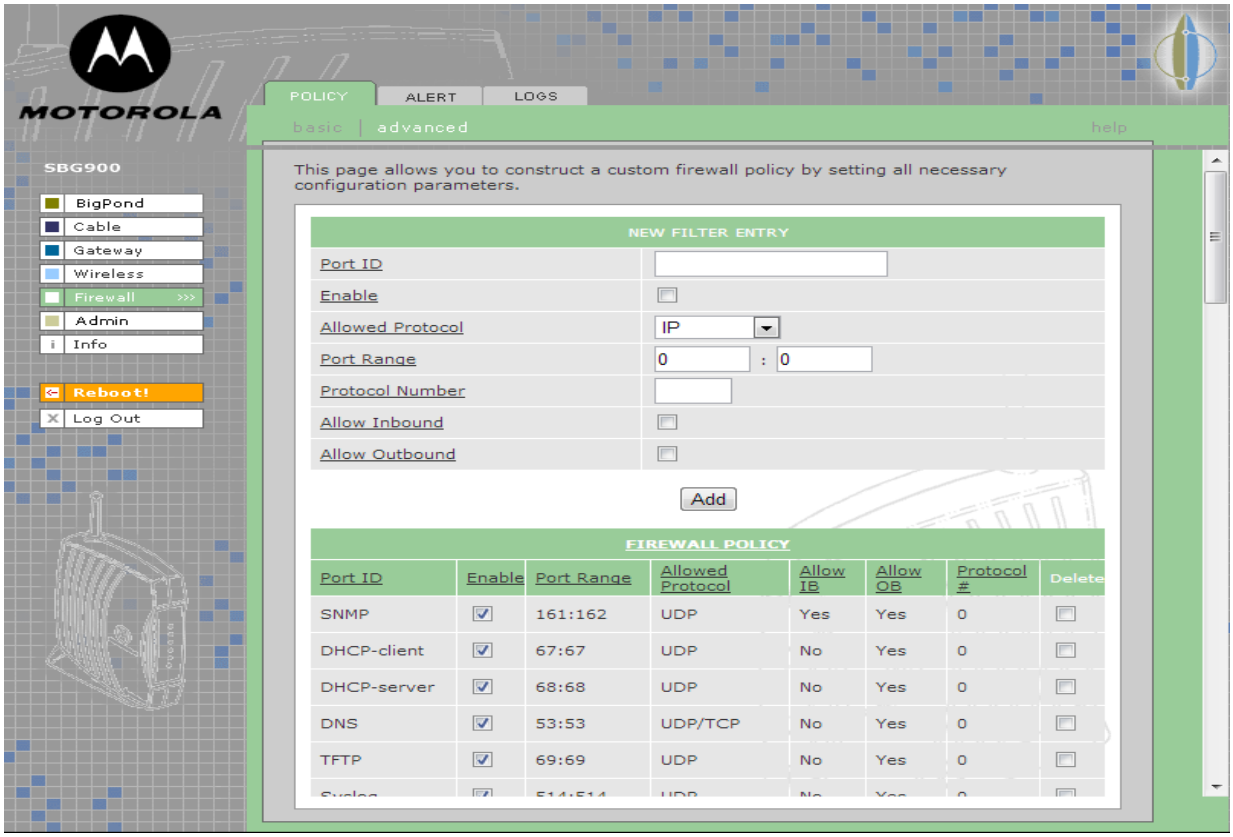
None:

Desabilita o firewall. Para habilitar uma fácil configuração de rede, é o padrão. Depois de configurar sua rede, use High, Medium ou Low para melhorar sua segurança.

5 Clique em **Apply** para aplicar suas mudanças.

Firewall > POLICY – página “advanced”

Para criar uma política de firewall customizada, primeiro selecione **Custom** e clique em **Apply** em Firewall > POLICY – página básica. Então use essa página para configurar uma política de firewall customizada.



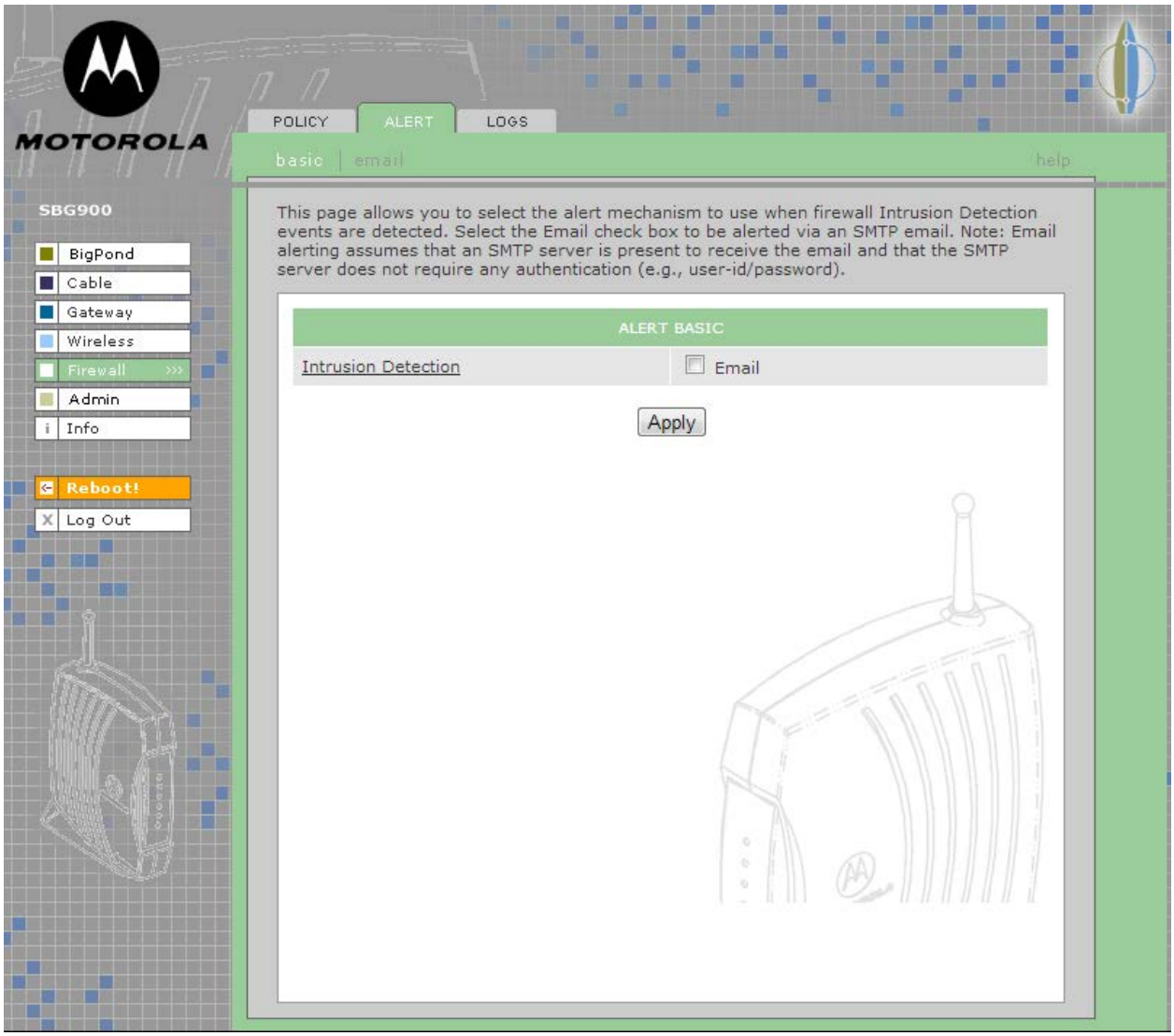
Para basear a política customizada em um modelo predefinido, escolha High, Medium ou Low mais embaixo, no campo **Policy Template,** e clique em **Apply Policy Template.**

Firewall > POLICY – campos da página “advanced”

Campo	Descrição
NEW FILTER ENTRY	Secção da janela de política avançada onde pode-se construir um firewall customizado.
Port ID	O nome do protocolo sendo filtrado.
Enable	Marque essa caixa para habilitar a filtragem da política do firewall para essa porta.
Allowed	Os protocolos permitidos.
Port Range (From:To)	Define o alcance da porta, que deve conter todas as portas requeridas pelo protocolo.
Protocol Number	O número do protocolo dos pacotes IP a serem permitidos.
Allow Inbound	Filtra os dados de entrada vindos da Internet nas portas especificadas.
Allow Outbound	Filtra os dados de saída para a Internet nas portas especificadas. Uma inspeção inteligente garante respostas apropriadas para sessões Outbound.
Add	Clique para adicionar o novo filtro, que estará exibido na aba FIREWALL POLICY (logo abaixo).
FIREWALL POLICY table	Lista as políticas de firewall.
Enable	Marque essa caixa para habilitiar a filtragem da política de firewall para a porta.
Delete	Selecione a caixa Delete para deletar o filtro.
Apply	Clique para aplicar suas mudanças.
FIREWALL POLICY TEMPLATE	Te permite selecionar um modelo de política de firewall predefinido no qual basear sua política customizada – High, Medium or Low.
Apply Policy Template	Clique para aplicar os modelos de política de firewall predefinidos e cancelar qualquer customização.

Firewall > ALERT – página “basic”

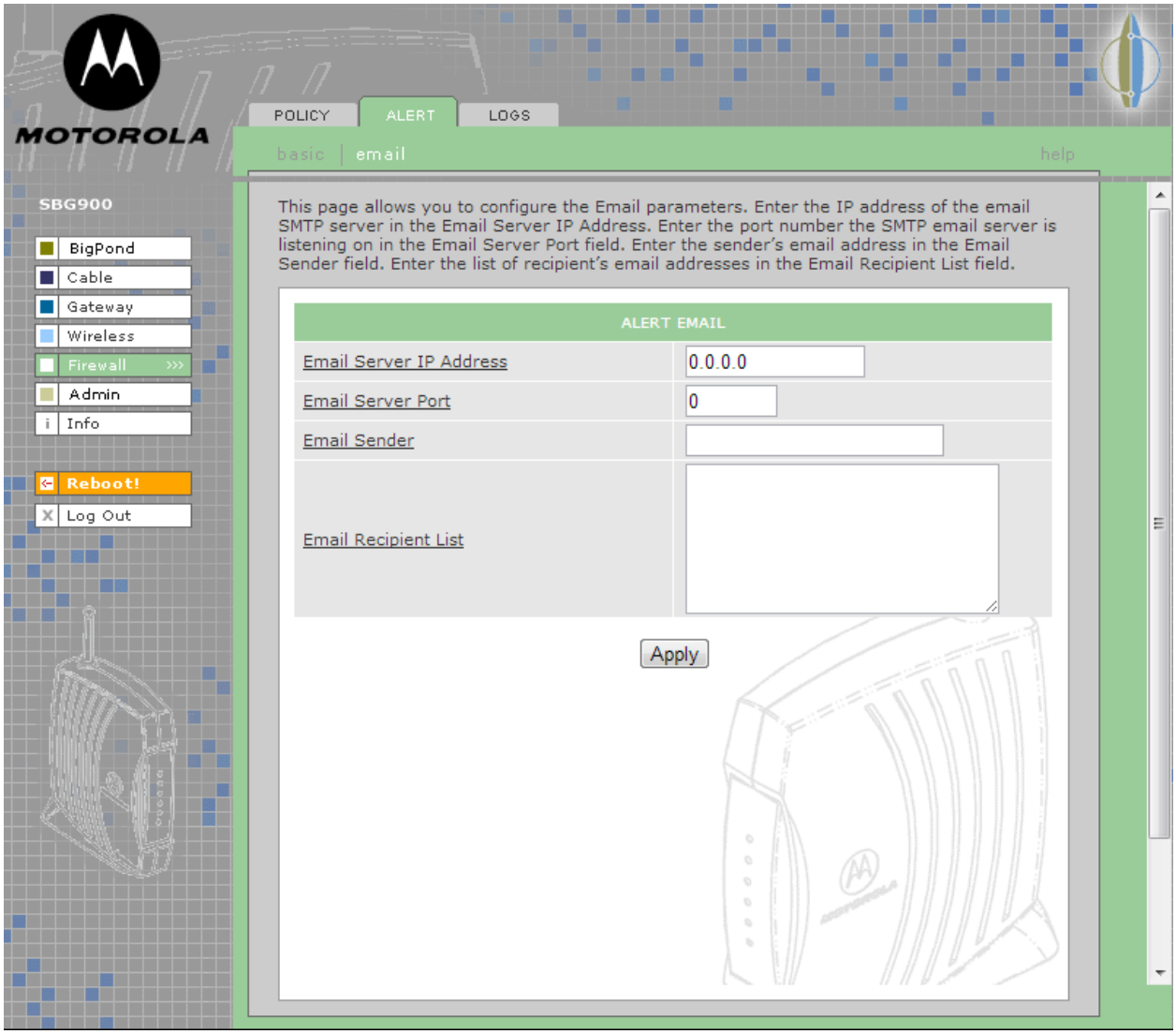
Pode-se usar essa página para definir o mecanismo de alerta para eventos de detecção de intrusão no firewall.



Firewall > ALERT – campos da página “basic”

Campo	Descrição
Intrusion Detection	Marque a caixa **Email** para ser alertado via e-mail SMTP. Um servidor SMTP que não requer nenhuma autenticação como usuário ou senha deve ser apresentado para receber o e-mail.
Apply	Clique para aplicar suas mudanças.

Firewall > ALERT – página “email”

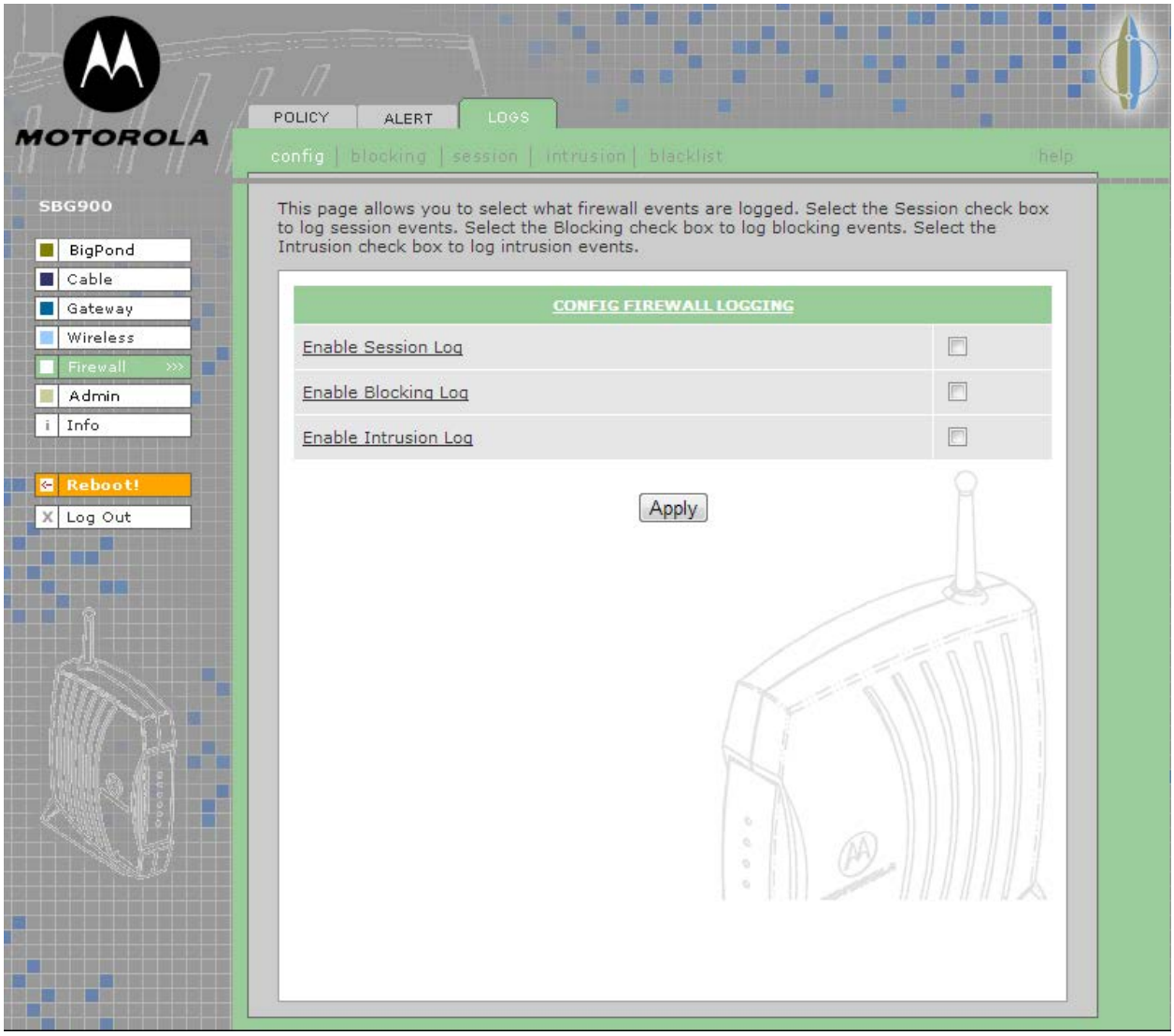


Firewall > ALERT – campos da página “email”

Campo ou Botão	Descrição
E-mail Server IP Address	Define o endereço IP do servidor de e-mail em formato decimal com pontos.
E-mail Server Port	Define o número da porta do servidor de e-mail.
E-mail Sender	Define o endereço de e-mail do remetente.
E-mail Recipient List	Define a lista de endereços de e-mail que recebem alertas do firewall do SBG900.
Apply	Clique para aplicar suas mudanças.

Firewall > Página “LOGS”

Você pode usar essa página para definir quais eventos do firewall são registrados.



Firewall > LOGS – campos da página LOGS

Campo ou Botão	Descrição
Enable Session Log	Marque essa caixa para registrar eventos da sessão.
Enable Blocking Log	Marque essa caixa para registrar eventos de bloqueio.
Enable Intrusion Log	Marque essa caixa pra registrar intrusões.
Aplly	Clique para aplicar suas mudanças.

Firewall > LOGS

Opção	Descrição
Session Log	A Sessão Log mostra sessões de dados que ocorreram e foram rastreadas pelo Firewall. Para habilitar o registro de sessões, a opção **Enable Log Session** deve estar selecionada. Uma política de Firewall deve estar em efeito para eventos de sessão serem gerados. Se a política de firewall está selecionada em **None**, então nenhuma nova entrada de sessão será gerada.
Blocking Log	O Blocking Log mostra os eventos de bloqueio do firewall. Para habilitar o registro de eventos de bloqueio, a opção **Enable Blocking** Log deve estar selecionada. Uma política de Firewall deve estar em efeito para eventos de bloqueio serem gerados. Se a política de firewall está selecionada em **None**, então nenhuma nova entrada de sessão será gerada.
Intrusion Log	O blocking Log mostra as tentativas de intrusões que ocorreram e foram evitadas pelo firewall. Para habilitar o registro de intrusões, a opção **Enable Intrusion Log** deve estar selecionada. Uma política de Firewall deve estar em efeito para eventos de bloqueio serem gerados. Se a política de firewall está selecionada em **None**, então nenhuma nova entrada de sessão será gerada.
Blacklist	A **Blacklist** (lista negra) mostra os endereços IP que foram determinados pelo firewall por terem quebrado a política do firewall do SBG900. Uma política de Firewall deve estar em efeito para eventos de bloqueio serem gerados. Se a política de firewall está selecionada em **None**, então nenhuma nova entrada de sessão será gerada.

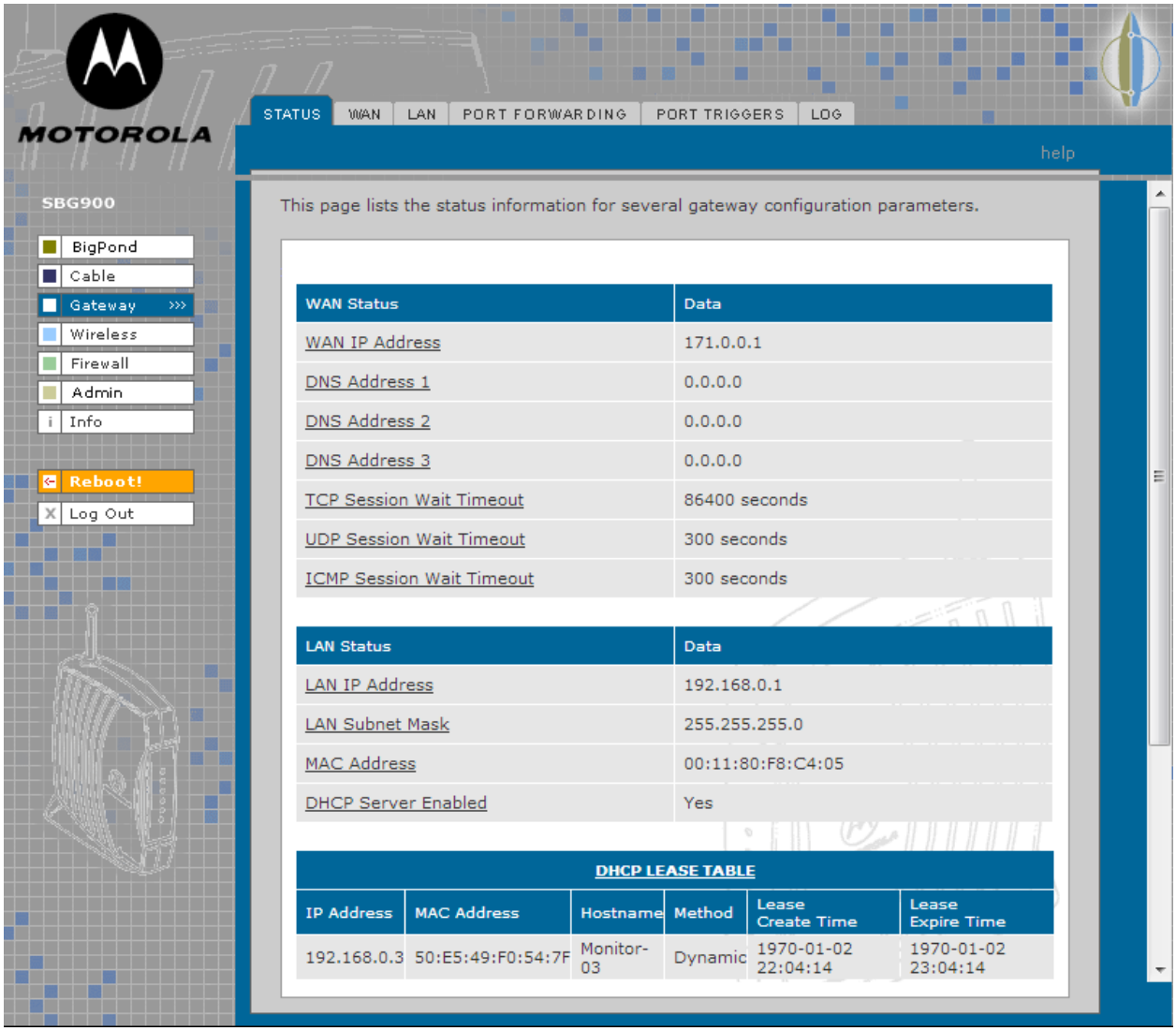
❖ Configurando o Gateway

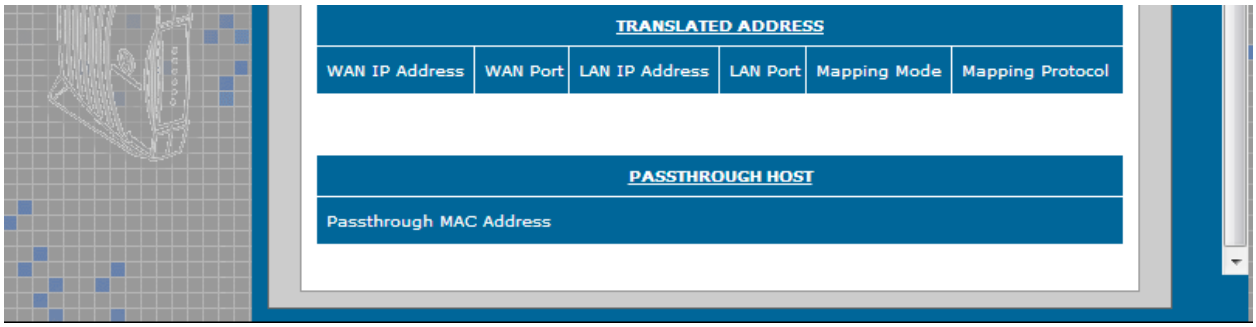
Esta sessão descreve as páginas de configuração do Gateway no programa de configuração do SBG900.

- Gateway > Página STATUS
- Gateway > Página WAN
- Gateway> LAN – Página “nat config”
- Gateway > LAN – Página “dhcp server config”
- Gateway > LAN – Página “dhcp leases”
- Gateway > PORT FORWARDING – Página “status”
- Gateway > PORT FORWARDING – Página “config”
- Gateway > PORT TRIGGERS – Página “predefined”
- Gateway > PORT TRIGGERS – Página “custom”
- Gateway > Página “LOG”

Gateway > Página “STATUS”

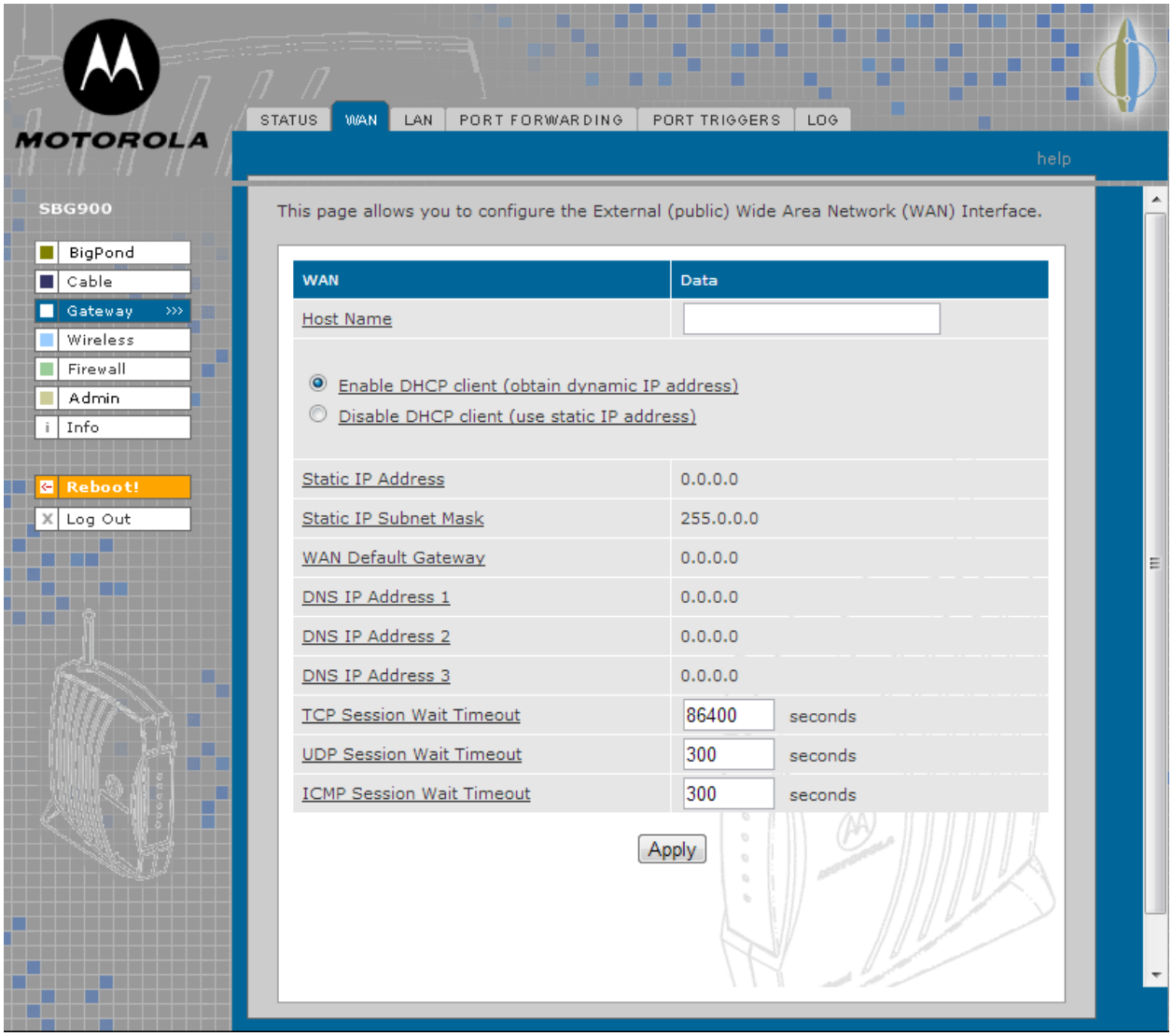
Esta página mostra a informação de status do gateway:





Gateway > Página “WAN”

Use esta página para configurar a interface externa (pública) da WAN.



Gateway > campo da página “WAN”

Campo	Descrição
Host Name	Se o provedor de serviço a cabo solicitar um nome de usuário para acessar sua rede, digite-o neste campo. O padrão é **None**.
Enable DHCP Client	Habilitar o cliente DHCP faz com que o gateway sem fio automaticamente obtenha o endereço IP público, máscara de sub-rede, nome de domínio e servidor(es) DNS. Mais comumente, o cliente DHCP está ativo se o provedor de serviço a cabo automaticamente designar um endereço IP público de seu servidor DHCP. Habilitar o cliente DHCP é o padrão.

Disable DHCP Cliente Se o provedor de serviço a cabo não designa automaticamente um endereço IP usando DHCP, eles devem prover um endereço IP estático. Quando você desativa o cliente DHCP, você deve digitar o endereço IP estático, máscara de sub-rede, servidor(es) DNS e nome de domínio (se necessário) nos campos dispostos. Desativar o cliente DHCP é desligado por padrão.

Static IP Address Se a opção de desativar o cliente DHCP está habilitada, digite o endereço IP estático fornecido pelo provedor de serviço a cabo em formato decimal com pontos. O padrão é **None.**

Static IP Subnet Mask Se a opção de desativar o cliente DHCP está habilitada, digite a máscara de sub-rede associada ao endereço de IP estático em formato decimal com pontos. O padrão é **None**.

WAN Default Gateway Quando se está usando um endereço IP designado estaticamente pelo seu ISP, digite o gateway padrão com o qual o SBG deveria estar usando para se comunicar na WAN.

DNS IP Address 1/2/3 O servidor DNS do provedor de serviço a cabo fornece um endereço de resolução nome-para-IP. Se o provedor de serviço a cabo não designar automaticamente endereços DNS de seu servidor DHCP, eles devem fornecer pelo menos um endereço IP de servidor DNS para digitar nesses campos em formato decimal com pontos. O padrão é **None**.

TCP Session Wait Timeout Seleciona o tempo máximo em segundos a esperar antes de assumir que uma sessão TCP se esgotou. O padrão é 24 horas.

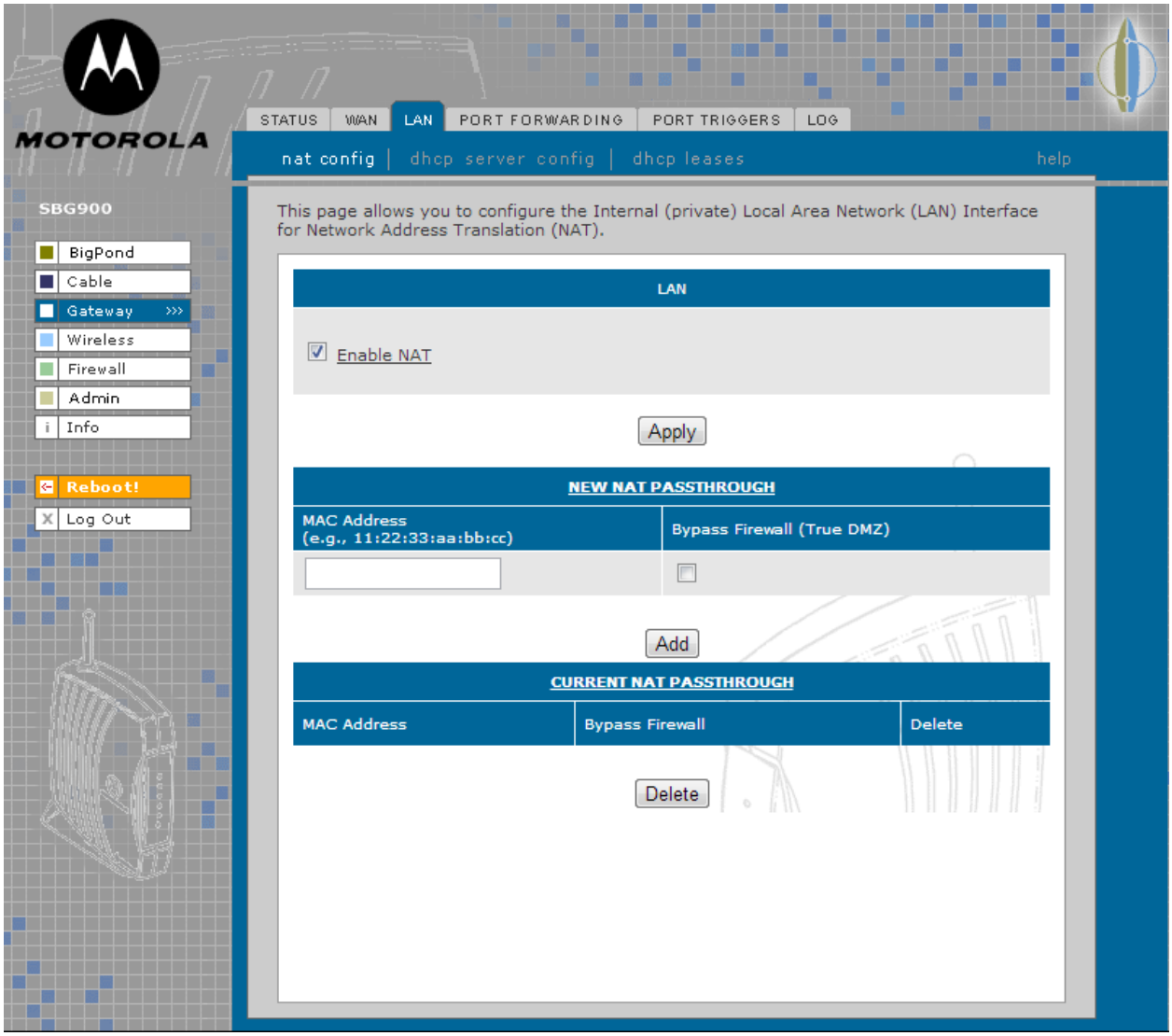
UDP Session Wait Timeout Seleciona o tempo máximo em segundos a esperar antes de assumir que uma sessão UDP se esgotou. O padrão é 300 segundos (5 minutos).

ICMP Session Wait Timeout Seleciona o tempo máximo em segundos a esperar antes de assumir que uma sessão ICMP se esgotou. O padrão é 300 segundos (5 minutos).

Apply Clique para aplicar suas mudanças.

Gateway > LAN – Página “nat config”

Use esta página para habilitar NAT e adicionar clientes à lista CURRENT NAT PASSTHROUGH:



Gateway > LAN – campos da página “nat config”

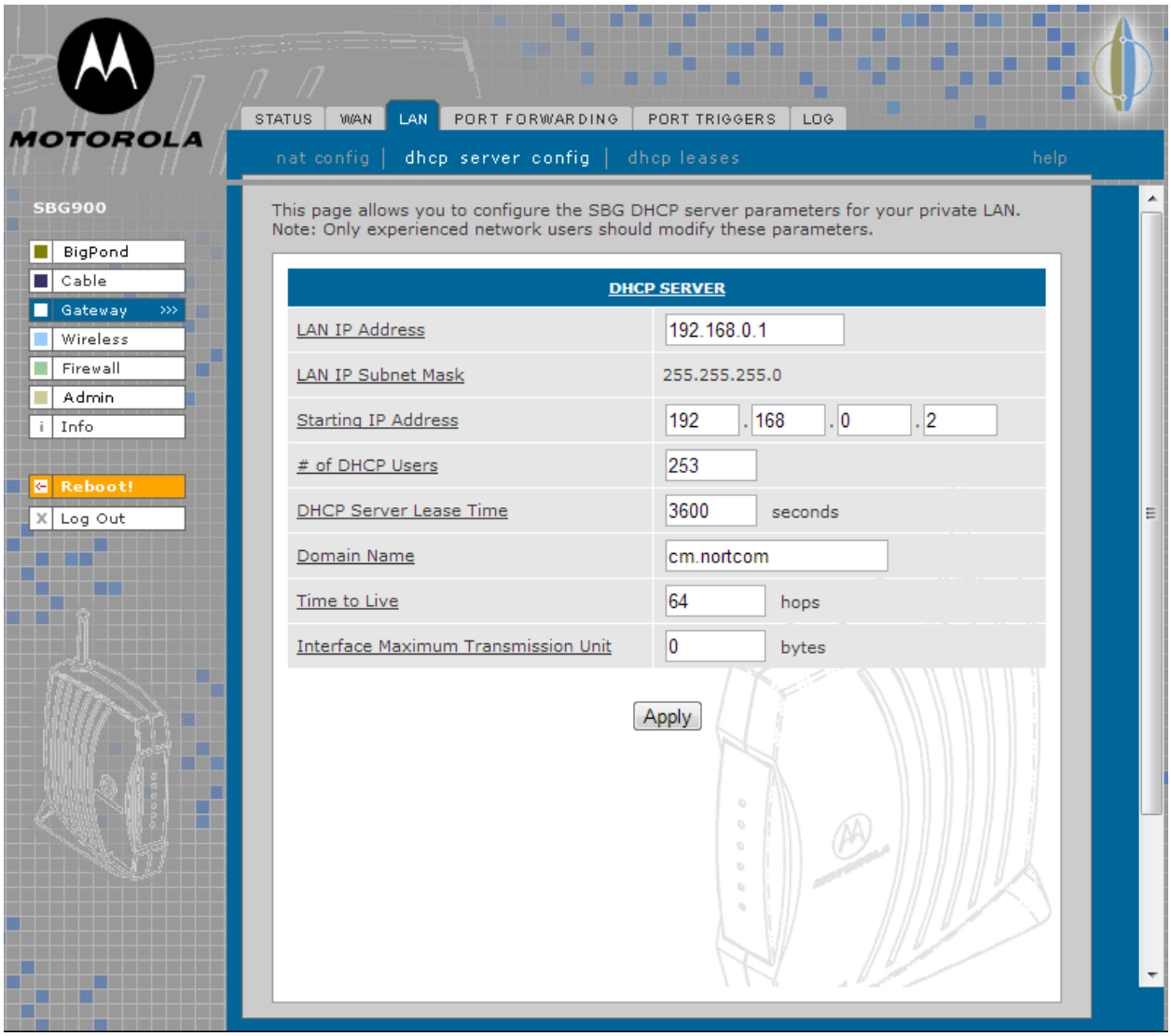
Campo ou Botão	Descrição
LAN	
Enable nat	Se habilitado, o único endereço IP designado pelo provedor de serviço a cabo é mapeado para muitos endereços IP pelo SBG900. Após habilitar, deve-se reiniciar o SBG900.
NEW NAT PASSTHROUGH	Especifica até 32 computadores exceção não submetidos ao NAT, usando seus endereços MAC.
MAC Address	Digite o endereço MAC do cliente exceção. O formato é 16 numerais hexadecimais.

Gateway > LAN – campos da página “nat config” (continuação)

Bypass Firewall (True DMZ)	Marque essa para selecionar o computador exceção NAT como um cliente DMZ. Use esta configuração com extremo cuidado, pois um cliente DMZ é completamente aberto a hackers de internet.
Add	Clique para adicionar o endereço MAC à lista CURRENT NAT PASSTHROUGH.
CURRENT NAT PASSTHROUGH	Lista os computadores da LAN que estão configurados como exceções NAT.
Delete	Clique para deletar o endereço MAC selecionado da lista de exceções NAT.

Gateway > LAN – Página “dhcp server config”

Apenas administradores experientes de redes devem usar essa página para realizar configurações do servidor DHCP avançado.



Gateway > LAN – campos da página “dhcp server config”

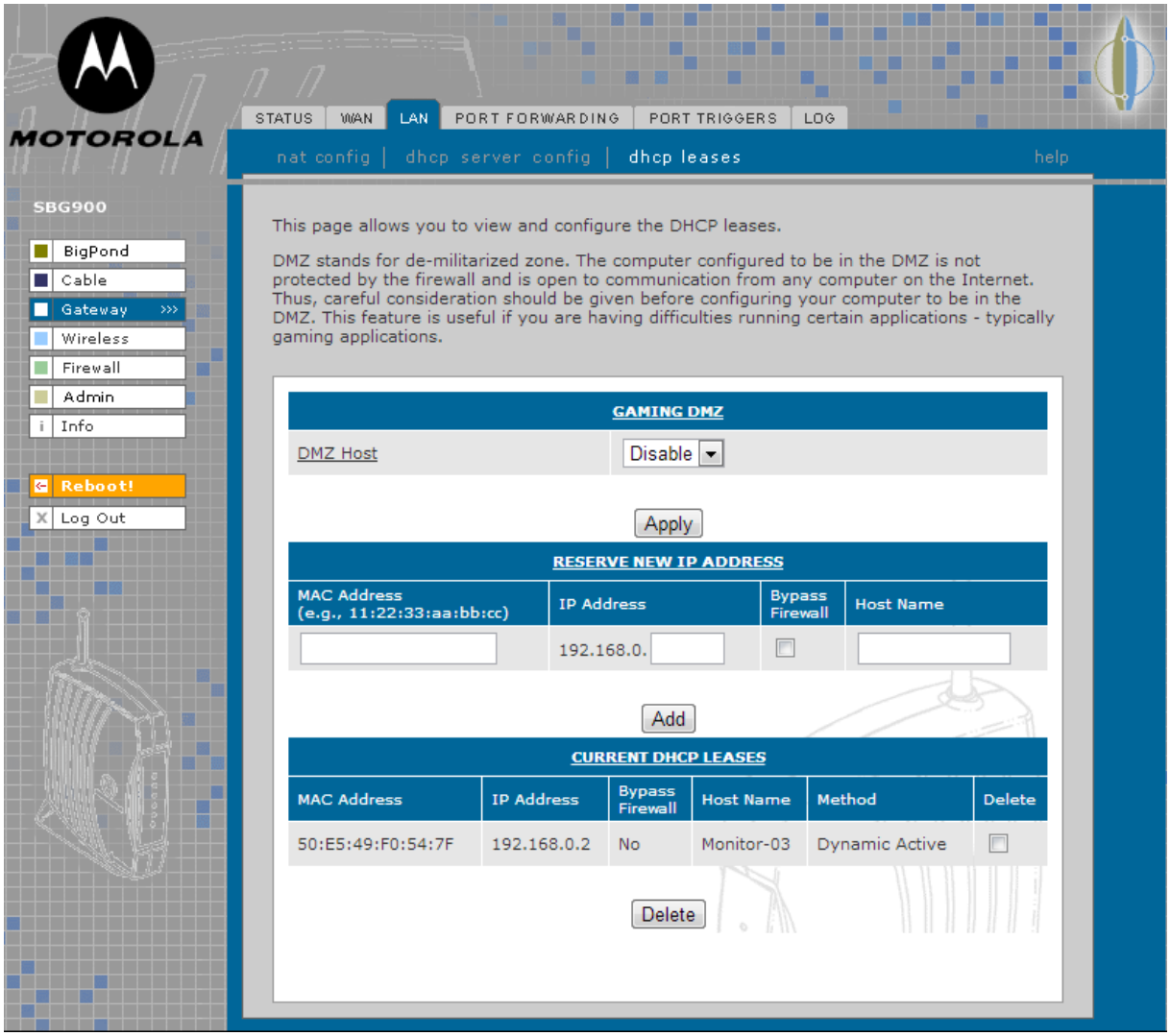
Campo	Descrição
LAN IP Address	Digite o endereço IP do SBG900 para sua LAN privada. O padrão é 192.168.0.1.
LAN IP Subnet Mask	A máscara de sub-rede. O Padrão é 255.255.255.0.
Starting IP Address	Digite o endereço IP inicial a ser atribuído pelo servidor DHCP do SBG900 para os clientes. O padrão é 192.168.0.2.
# of DHCP Users	Seleciona o número de clientes para o servidor DHCP do SBG900 atribuir um endereço IP privado. Existem 253 possíveis endereços de clientes. O padrão é 253.
DHCP Server Lease Time	Seleciona o tempo em segundos em que o servidor DHCP do SBG900 libera um endereço IP para um cliente. O padrão é 3600 segundos (60 minutos).

Gateway > LAN –campos da página “dhcp server config” (continuação)

Campo	Descrição
Domain Name	Define o nome de domínio para a LAN do SBG900. O padrão é **None**.
Time to Live	Define o TTL (limite de saltos) para pacotes de saída. O padrão é 64.
Interface Maximum Transmission Unit	Define o MTU da LAN do SBG900 em bytes. O mínimo é 68 bytes e o padrão é 1500 bytes.
Aplly	Clique para aplicar suas mudanças. Você deve reiniciar o SBG900.

Gateway > LAN – página “dhcp leases”

Use esta página para configurar as concessões do DHCP.



Gateway > LAN – campos da página “dhcp leases”

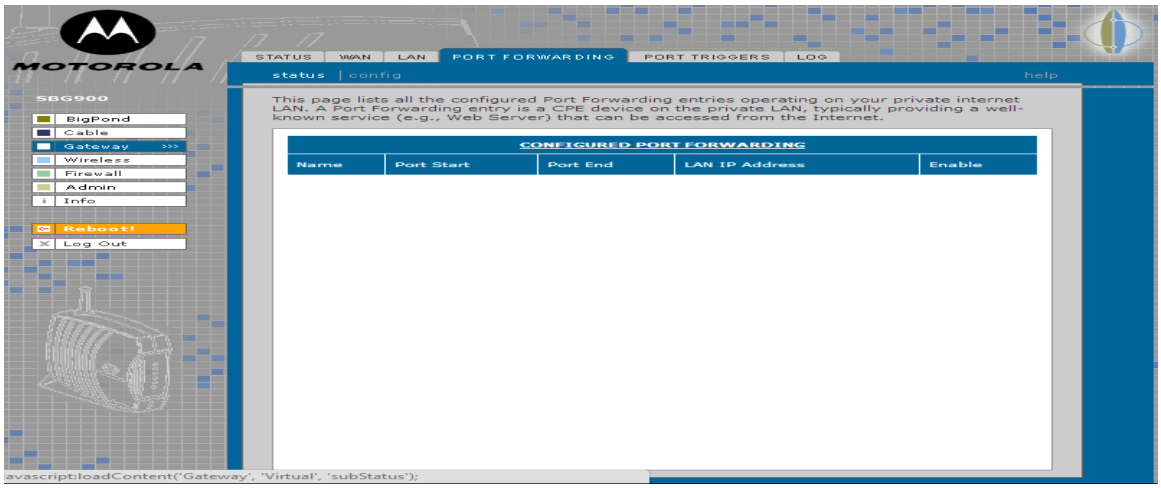
Campo	Descrição
Enable Gaming DMZ	Marque essa caixa para designar os computadores ou aparelhos de jogos selecionados como o hospedeiro DMZ. Isso pode ser útil se você tiver dificuldades em rodar certas aplicações; tipicamente aplicações de jogos.
(Gaming) DMZ Host	O hospedeiro DMZ de jogos é um computador com um endereço IP reservado designado como o hospedeiro DMZ padrão. Somente um hospedeiro DMZ pode estar ativo por vez. O hospedeiro DMZ não é protegido pelo firewall, estando aberto a comunicações ou infiltrações de qualquer computador da internet. Considere cuidadosamente antes de configurar um computador para estar no DMZ. O benefício de usar um hospedeiro DMZ de jogos ao invés de uma exceção NAT, é que um hospedeiro DMZ de jogos não requer um endereço IP público como na exceção NAT.

Gateway > LAN – campos da página “dhcp leases”

Campo	Descrição
RESERVE NEW IP ADDRESS	Você pode reservar até 32 endereços IP atribuídos pelo servidor DHCP do SBG900 para clientes específicos da LAN. Por exemplo, para garantir que eles sempre recebam o mesmo endereço IP privado, você pode reservar endereços IP para um servidor FTP privado ou dispositivo DMZ de jogos.
MAC Address	Digite o endereço MAC do cliente DHCP para o qual um endereço IP reservado é requerido.
IP Address	Define a porção do hospedeiro de endereços IP reservados para os clientes da LAN que tem o endereço MAC especificado. Quando o cliente da LAN solicitar um endereço IP, o servidor DHCP do SBG900 atribui para esse cliente este endereço IP.
Host Name	Se o seu provedor de internet solicitar o um nome de usuário para acessar sua rede, digite o nome de usuário fornecido a você, no campo **Host Name**.
Add	Clique em **Add** para reservar um novo endereço IP.
CURRENTLY RESERVED IP ADRESSES	Exibe todos os clientes do DHCP que têm endereços IP reservados.
Mac Address	Exibe o endereço MAC do cliente.
IP Address	Exibe seu endereço IP reservado.
Host Name	Exibe seu nome de hospedeiro.
Method	Exibe o status de atribuição dinâmica e estática. Adicione ou delete atribuições dinâmicas e estáticas nesse campo.
Delete	Clique nesta caixa para remover o endereço IP reservado para o cliente.
Delete	Clique neste botão para remover os endereços de IP reservados para clientes designados pela caixa **Delete**.

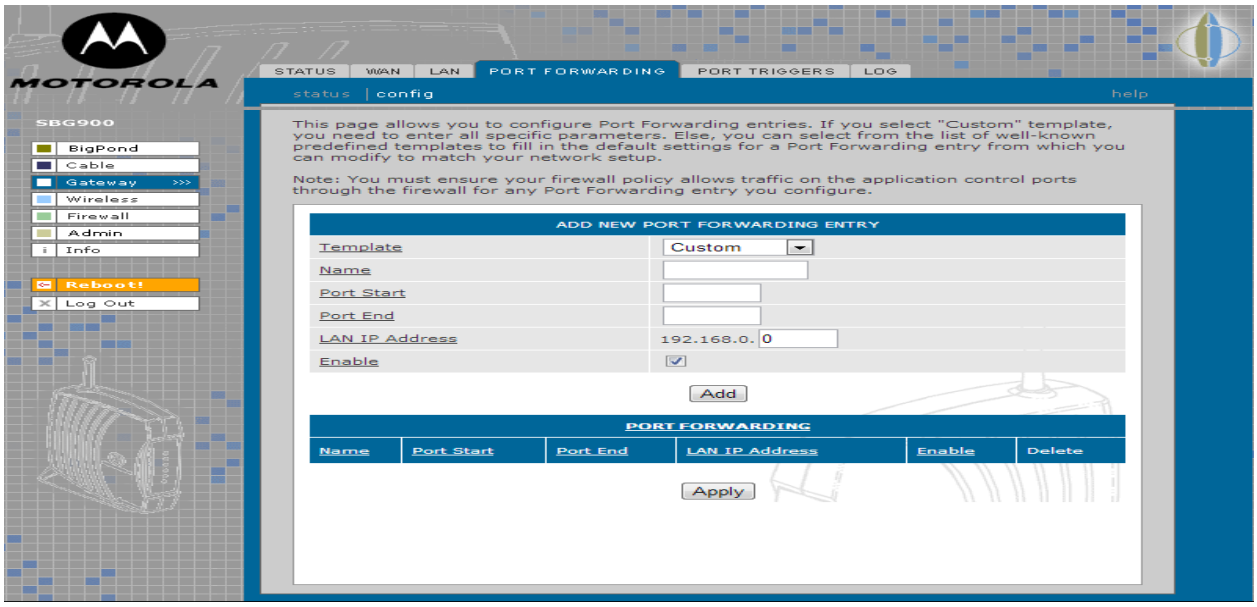
Gateway > PORT FORWARDING – Página “status”

Use esta página para exibir os encaminhamentos de porta configurados na LAN do SBG900. Os campos são os mesmos do **Gateway > PORT FORWARDING – página “config”**:



Gateway > PORT FORWARDING – Página “config”

Use esta página para configurar até 32 servidores virtuais.



Gateway > PORT FORWARDING – Campos da página “config”

Campo	Descrição
ADD NEW PORT FORWARDING ENTRY	Você pode configurar até 32 servidores virtuais.
Template	Se você selecionar **Custom**, deve definir o **Name**, **Port Start**, **Port End** e **LAN IP Address**. Se você selecionar um modelo predefinido tal como HTTP ou FTP, os valores de **Name**, **Port Start**, **Port End** são providos. Você só precisa digitar o LAN IP Address (endereço ip da LAN), e mudar os valores padrão, caso necessário.
Name	Digite um único identificador para o servidor virtual customizado. A prática usual é usar o protocolo como único identificador (por exemplo **ftp**).
Port Start	Define a porta de interface interna da LAN ou o início do alcance de uma porta. Requisições de conexão da entrada de internet são estaticamente mapeadas para essa porta.
Port End	Se um alcance de portas é requerido, define o final do alcance dela.
LAN IP Address	Define o endereço IP privado da LAN para a página **port forwarding**. Um usuário da internet deve conhecer o endereço IP público para acessar qualquer entrada de encaminhamento de porta que você define na LAN privada.
Enable	Marque esta caixa para habilitar as entradas de encaminhamento de porta para serem acessados através do NAT.
Add	Clique para adicionar o servidor virtual à lista PORT FORWARDING.
PORT FORWARDING	Exibe os servidores virtuais customizados configurados.

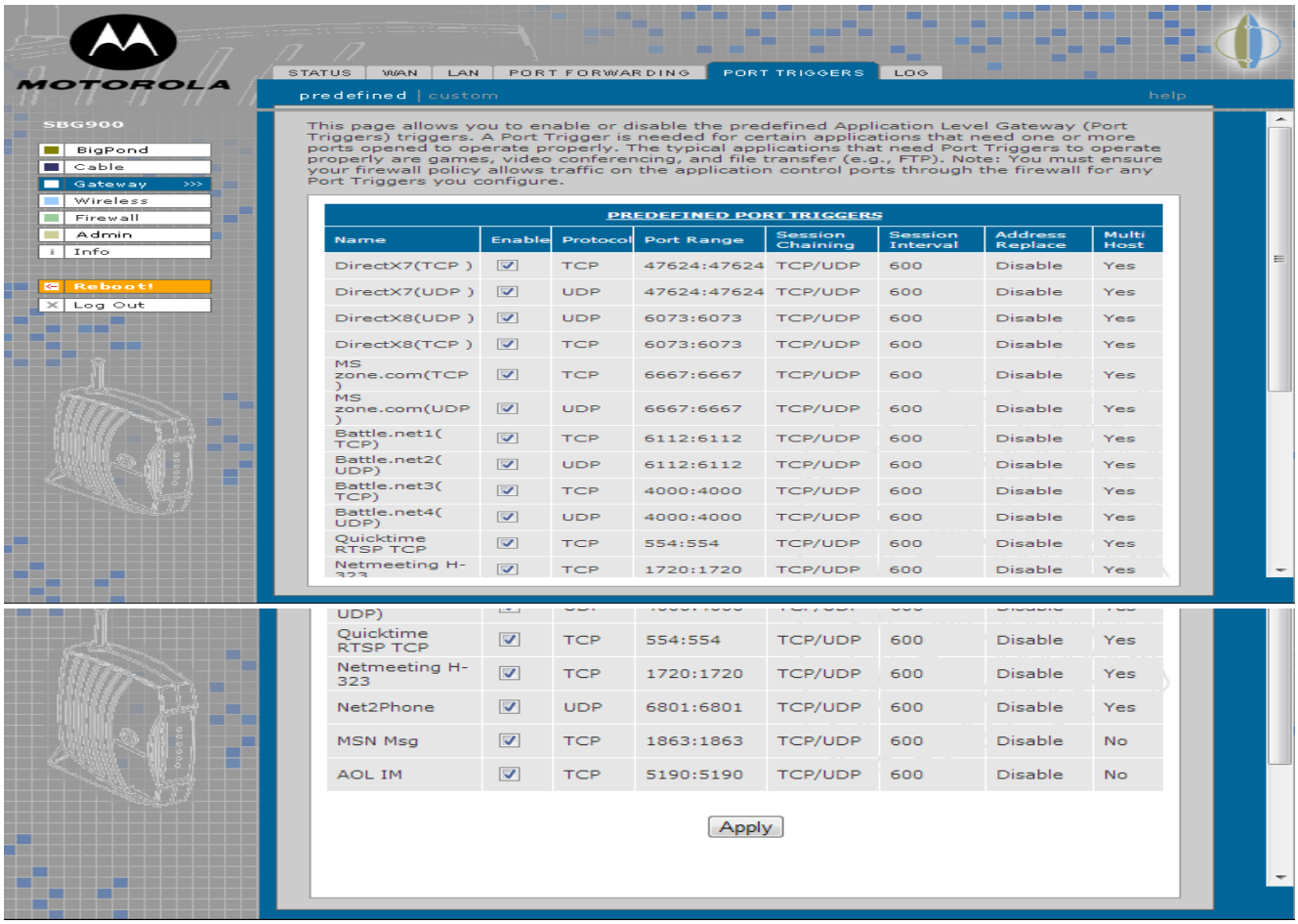
Gateway > PORT TRIGGERS – Página “predefined”

Quando você roda uma aplicação para computador que acessa a internet, isso se comunica com um computador na internet. Em algumas aplicações, especialmente em jogos, o computador na internet também se comunica com o seu. O SBG900 suporta a ativação de portas, pois o NAT não permite normalmente essas conexões de entrada.

O SBG900 é pré-configurado com a ativação de portas para aplicações comuns. Você pode também configurar ativações de portas adicionais se necessário. Configurar ativação de portas para uma aplicação requer:

- O protocolo de transporte da aplicação – TCP ou UDP;
- O número da porta da aplicação.

Você pode usar os valores padrão para os parâmetros remanescentes.
Somente um PC por vez conectado ao SBG900, pode usar uma aplicação que requer ativação de portas. Use essa página para ver acionamentos de portasa predefinidos:

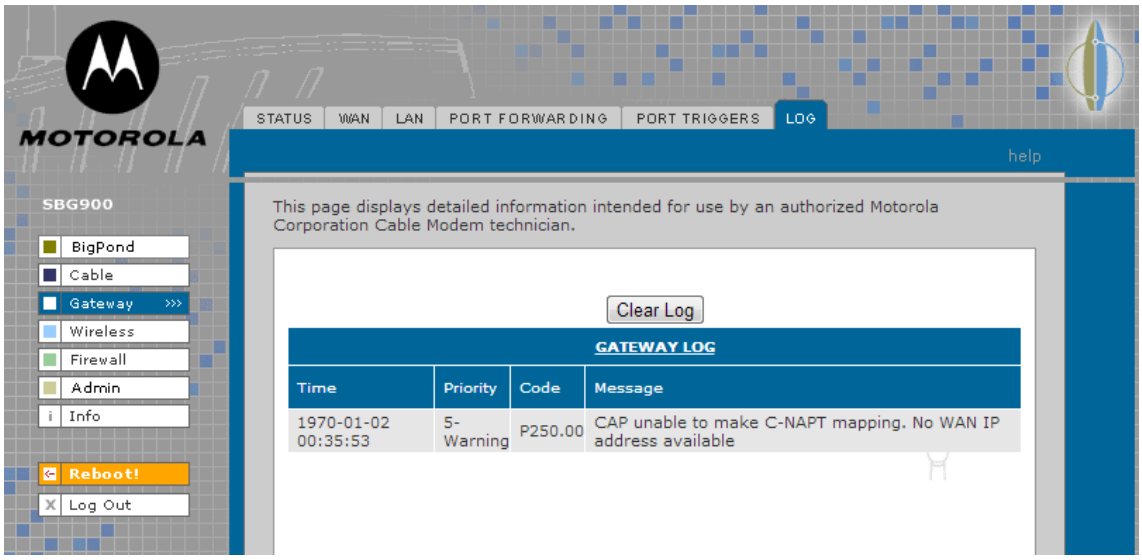

MOTOROLA
SBG900
BigPond
Cable
Gateway
Wireless
Firewall
Admin
Info
Reboot!
Log Out
STATUS
WAN
LAN
PORT FORWARDING
PORT TRIGGERS
LOG
predefined | custom
help
This page allows you to enable or disable the predefined Application Level Gateway (Port Triggers) triggers. A Port Trigger is needed for certain applications that need one or more ports opened to operate properly. The typical applications that need Port Triggers to operate properly are games, video conferencing, and file transfer (e.g., FTP). Note: You must ensure your firewall policy allows traffic on the application control ports through the firewall for any Port Triggers you configure.
PREDEFINED PORT TRIGGERS
Name | Enable | Protocol | Port Range | Session Chaining | Session Interval | Address Replace | Multi Host
DirectX7(TCP) | TCP | 47624:47624 | TCP/UDP | 600 | Disable | Yes
DirectX7(UDP) | UDP | 47624:47624 | TCP/UDP | 600 | Disable | Yes
DirectX8(UDP) | UDP | 6073:6073 | TCP/UDP | 600 | Disable | Yes
DirectX8(TCP) | TCP | 6073:6073 | TCP/UDP | 600 | Disable | Yes
MS zone.com(TCP) | TCP | 6667:6667 | TCP/UDP | 600 | Disable | Yes
MS zone.com(UDP) | UDP | 6667:6667 | TCP/UDP | 600 | Disable | Yes
Battle.net1(TCP) | TCP | 6112:6112 | TCP/UDP | 600 | Disable | Yes
Battle.net2(UDP) | UDP | 6112:6112 | TCP/UDP | 600 | Disable | Yes
Battle.net3(TCP) | TCP | 4000:4000 | TCP/UDP | 600 | Disable | Yes
Battle.net4(UDP) | UDP | 4000:4000 | TCP/UDP | 600 | Disable | Yes
Quicktime RTSP TCP | TCP | 554:554 | TCP/UDP | 600 | Disable | Yes
Netmeeting H-323 | TCP | 1720:1720 | TCP/UDP | 600 | Disable | Yes
Net2Phone | UDP | 6801:6801 | TCP/UDP | 600 | Disable | Yes
MSN Msg | TCP | 1863:1863 | TCP/UDP | 600 | Disable | No
AOL IM | TCP | 5190:5190 | TCP/UDP | 600 | Disable | No
Apply

Gateway > PORT TRIGGERS – Campos da página “predefined”

Campo	Descrição
ADD NEW SPECIAL	
APPLICATION	
Name	Exibe o nome único para os acionadores de porta. Isso é tipicamente o nome do protocolo.
Enable	Selecione a caixa **Enable** para ativar os acionadores de porta para as aplicações predefinidas.
Protocol	Exibe o protocolo de transporte para o acionadores de portas – TCP ou UDP.
Port Range	Exibe o alcance da porta (De/Para) para o acionador de portas.
Session Chaining	Exibe a seleção do encadeamento de sessão para o acionadores de porta – Disable, TCP ou TCP/UDP.
Session Interval	Exibe o intervalo da sessão definido para o acionador de porta.
Adress Replace	Exibe o método de reposicionamento de endereço para o acionador de portas.
Multi Host	Exibe a seleção de multi hospedeiro para o acionador de portas.
Add	Clique para adicionar o acionador de porta à PORT TRIGGERS TABLE.
PORT TRIGGERS TABLE	Lista todos os acionadores de portas que você definiu e seus parâmetros.
Priority Port	Seleciona a porta a ter status de prioridade.

Gateway> Página LOG

Use esta página para visualizar informações detalhadas sobre o gateway:



Gateway> LOG – Campos da página

Campo	Descrição
Time	A data e a hora no formato aaaa-mm-dd hh:mm:ss (hora hh é de 00 a 23).
Priority	Indica a importância da mensagem.
Code	Código associado a essa mensagem.
Message	Descreve o evento.

❖ Configurando TCP/IP

Você deve ter certeza de todos os computadores clientes estão configurados para TCP / IP (protocolo de comunicação entre computadores). Execute um dos seguintes:

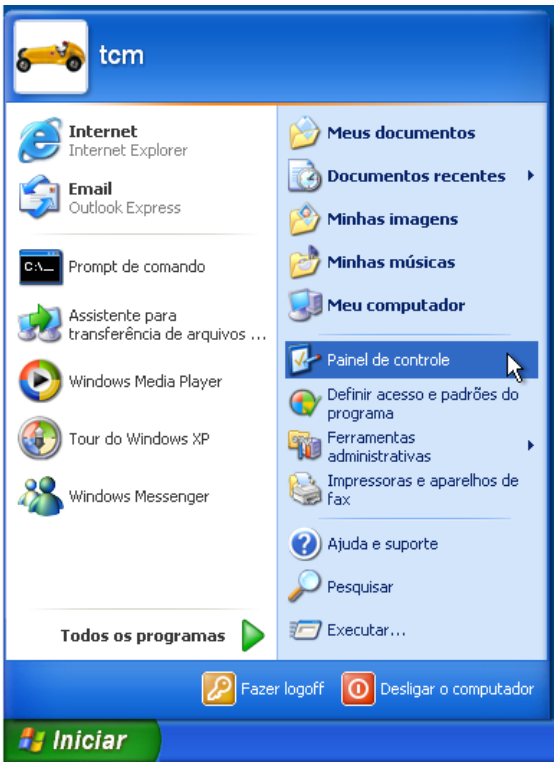
- Configurando o TCP/IP no Windows XP
- Siga as instruções no manual de usuário de seu Macintosh ou UNIX

Após configurar o TCP/IP, execute um dos seguintes procedimentos para verificar o endereço IP:

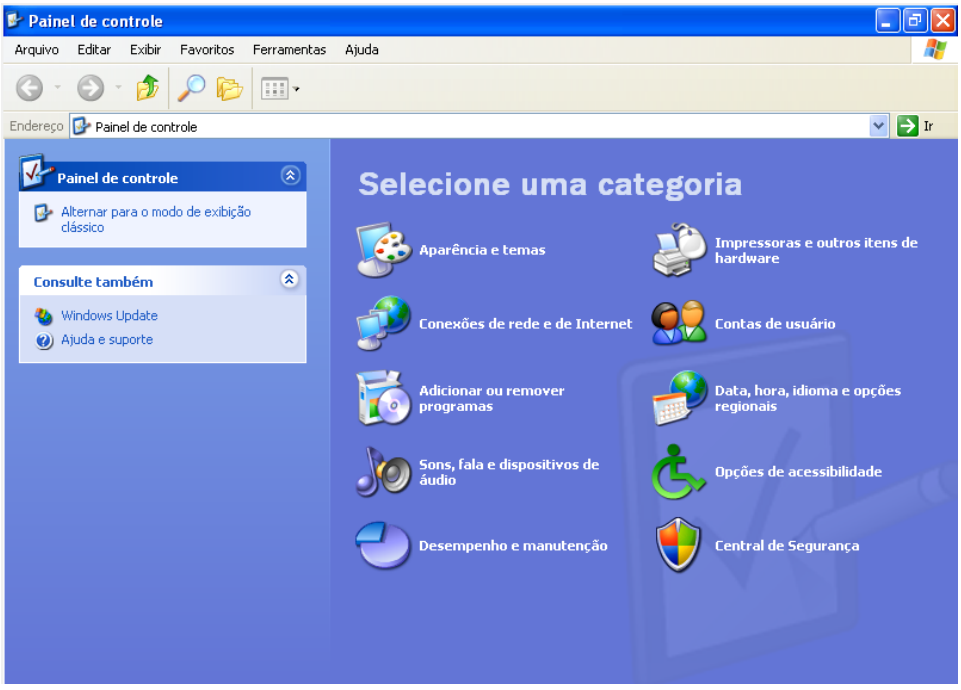
- Verificação do endereço IP no Windows XP
- Siga as instruções no manual de usuário de seu Macintosh ou UNIX

Configurando o TCP/IP no Windows XP

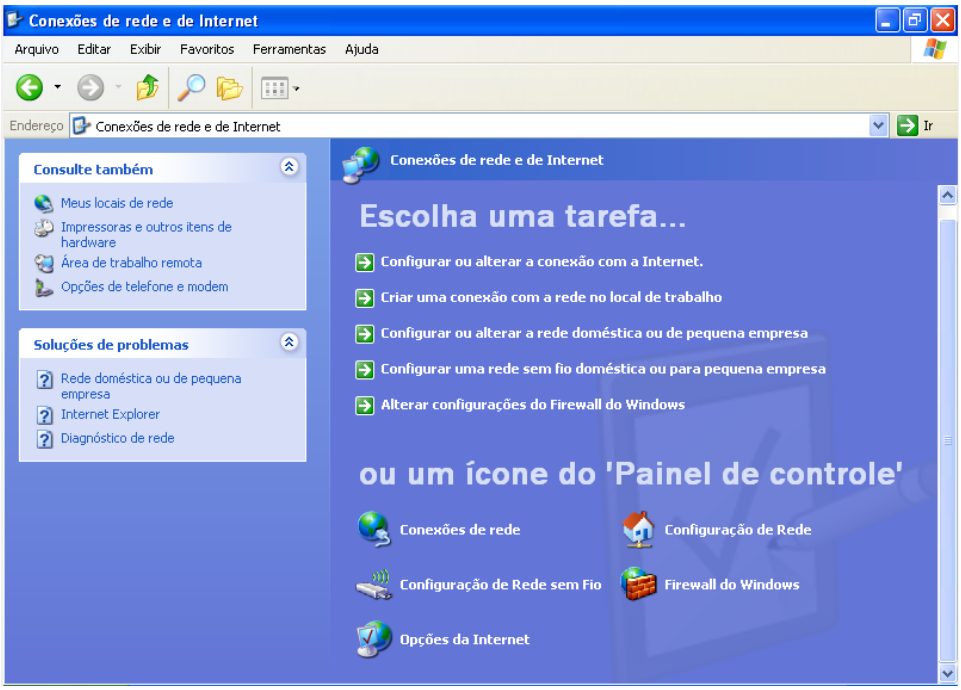
1. Na área de trabalho do Windows, clique em **Iniciar** para exibir a janela Iniciar:



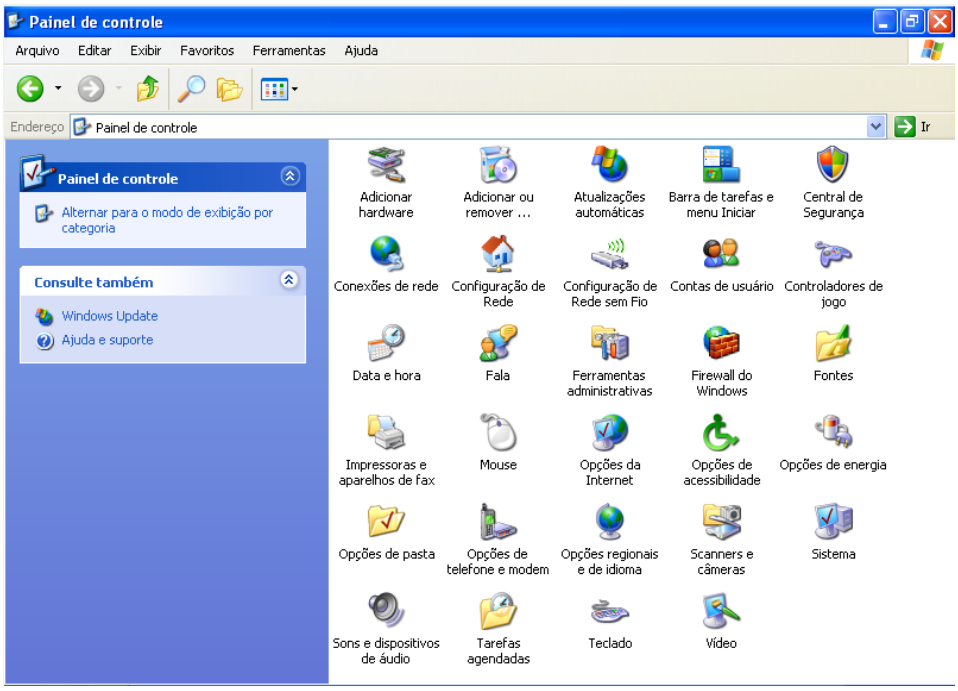
2. Clique em **Painel de Controle** para exibir a janela do Painel de Controle. A tela varia, dependendo do Windows XP, visualize as opções. Se a exibição for por categoria, conforme mostrado abaixo, continue com a etapa 3. Caso contrário, pule para ao passo 5.



3. Clique em **Conexões de Rede e Internet** para exibir a janela Conexões de Rede e Internet:

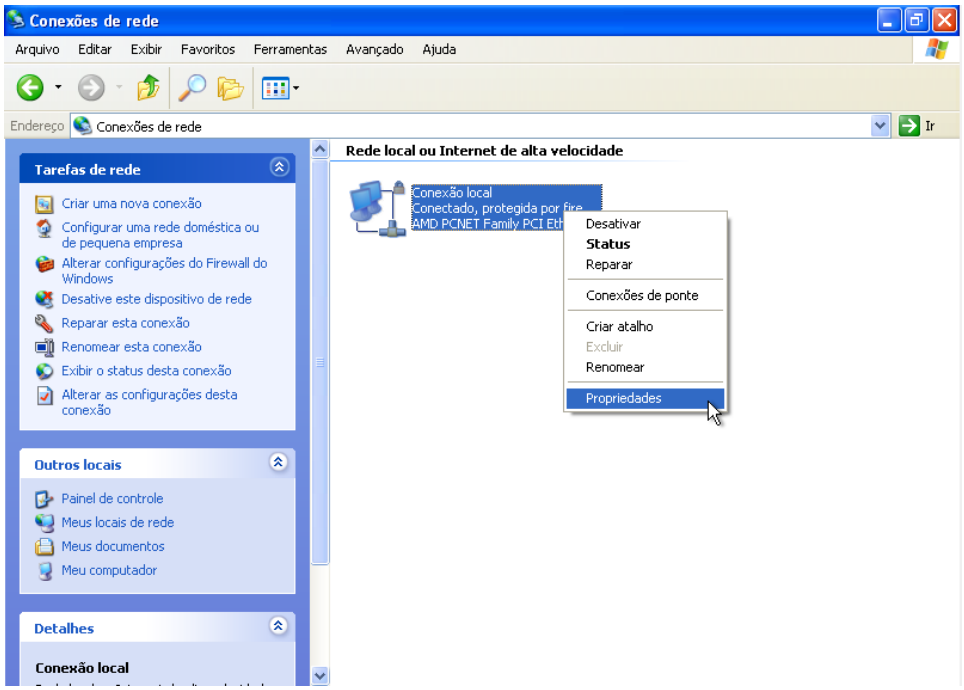

Conexões de rede e de Internet
Arquivo Editar Exibir Favoritos Ferramentas Ajuda
Endereço Conexões de rede e de Internet
Ir
Consulte também
Meus locais de rede
Impressoras e outros itens de hardware
Área de trabalho remota
Opções de telefone e modem
Soluções de problemas
Rede doméstica ou de pequena empresa
Internet Explorer
Diagnóstico de rede
Conexões de rede e de Internet
Escolha uma tarefa...
Configurar ou alterar a conexão com a Internet.
Criar uma conexão com a rede no local de trabalho
Configurar ou alterar a rede doméstica ou de pequena empresa
Configurar uma rede sem fio doméstica ou para pequena empresa
Alterar configurações do Firewall do Windows
ou um ícone do 'Painel de controle'
Conexões de rede
Configuração de Rede
Configuração de Rede sem Fio
Firewall do Windows
Opções da Internet

4. Clique em **Conexões de Rede** para exibir a LAN .
5. Se estiver no modo de exibição clássico será semelhante ao mostrado abaixo:

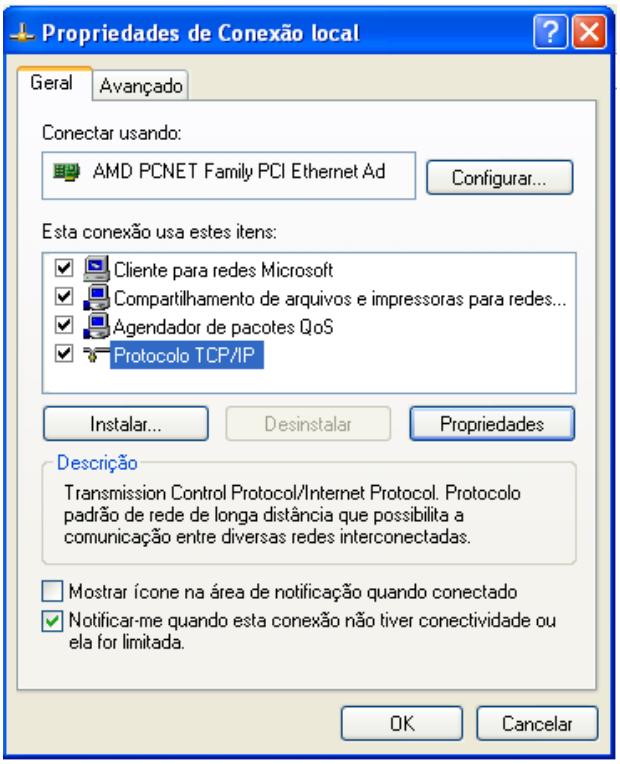


6. Clique em **Conexões de Rede** para exibir a LAN.

7. Clique com o botão direito do mouse na conexão de rede. Se mais de uma conexão for exibida, certifique-se de selecionar a conexão certa para sua interface de rede:

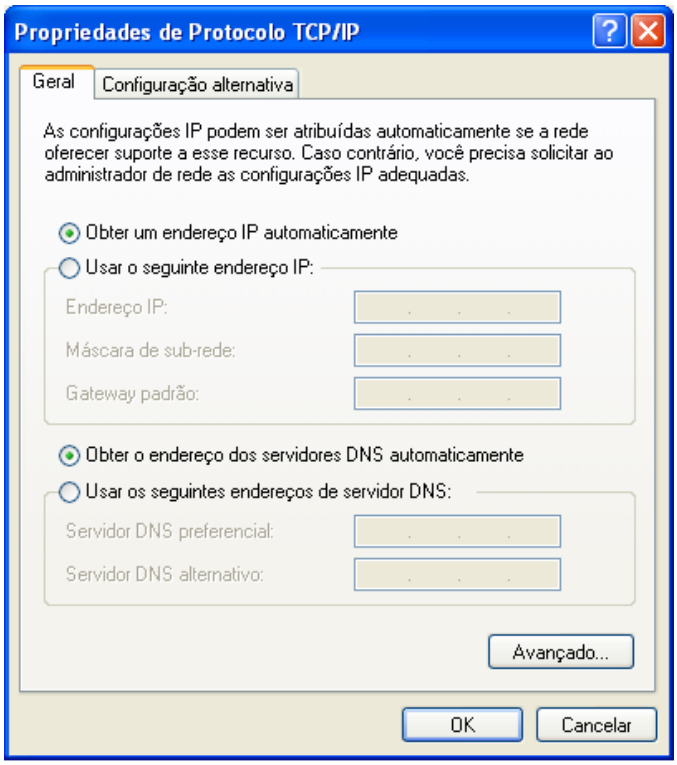


8. Selecione a opção **Propriedades** no menu para exibir a janela Propriedades de Conexão Local:


Propriedades de Conexão local
Geral
Avançado
Conectar usando:
AMD PCNET Family PCI Ethernet Ad
Configurar...
Esta conexão usa estes itens:
Cliente para redes Microsoft
Compartilhamento de arquivos e impressoras para redes...
Agendador de pacotes QoS
Protocolo TCP/IP
Instalar...
Desinstalar
Propriedades
Descrição
Transmission Control Protocol/Internet Protocol. Protocolo padrão de rede de longa distância que possibilita a comunicação entre diversas redes interconectadas.
Mostrar ícone na área de notificação quando conectado
Notificar-me quando esta conexão não tiver conectividade ou ela for limitada.
OK
Cancelar

9. Na janela Propriedades de Conexão Local, certifique-se de que Protocolo (TCP / IP) está marcada. Se não for selecionado, marque-a.

10. Selecione **Protocolo (TCP/IP)** e clique em **Propriedades** para exibir a janela Propriedades de Protocolo (TCP/IP):


Propriedades de Protocolo TCP/IP
Geral
Configuração alternativa
As configurações IP podem ser atribuídas automaticamente se a rede oferecer suporte a esse recurso. Caso contrário, você precisa solicitar ao administrador de rede as configurações IP adequadas.
Obter um endereço IP automaticamente
Usar o seguinte endereço IP:
Endereço IP:
Máscara de sub-rede:
Gateway padrão:
Obter o endereço dos servidores DNS automaticamente
Usar os seguintes endereços de servidor DNS:
Servidor DNS preferencial:
Servidor DNS alternativo:
Avançado...
OK
Cancelar

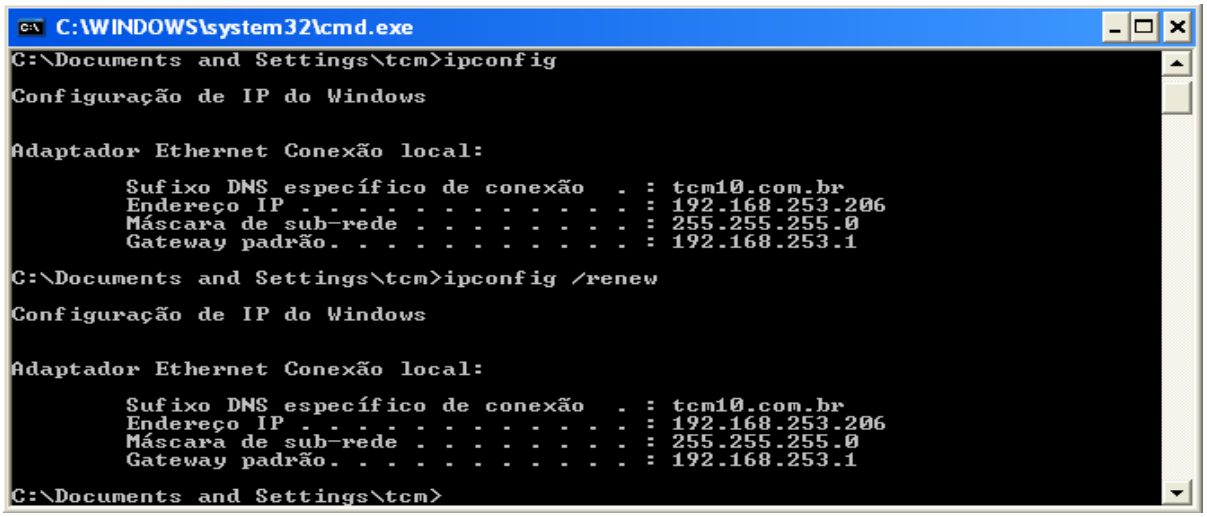
11. Verifique se as configurações estão corretas, como mostrado acima.
12. Clique em **OK** para fechar a janela Propriedades de TCP/IP.
13. Clique em **OK** para fechar a janela Propriedades de Conexão Local.

Quando você concluir a configuração TCP/IP, vá para "Verificação do endereço IP no Windows XP".

❖ Verificando o Endereço IP nos Windows XP e 7

Para verificar o endereço IP:

1. Na área de trabalho do Windows, clique em **Iniciar**.
2. Selecione **Executar**. A janela será aberta.
3. Digite **cmd** (sem aspas) e clique em **OK** para abrir a janela do prompt de comando.
4. Digite “ipconfig” (sem aspas) e aperte **ENTER** para exibir a configuração IP.


C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\tcm>ipconfig
Configuração de IP do Windows
Adaptador Ethernet Conexão local:
Sufixo DNS específico de conexão . : tcm10.com.br
Endereço IP . . . . . : 192.168.253.206
Máscara de sub-rede . . . . . : 255.255.255.0
Gateway padrão. . . . . : 192.168.253.1
C:\Documents and Settings\tcm>ipconfig /renew
Configuração de IP do Windows
Adaptador Ethernet Conexão local:
Sufixo DNS específico de conexão . : tcm10.com.br
Endereço IP . . . . . : 192.168.253.206
Máscara de sub-rede . . . . . : 255.255.255.0
Gateway padrão. . . . . : 192.168.253.1
C:\Documents and Settings\tcm>

Como Renovar o Endereço IP

Para renovar o endereço IP:

1. Digite “ipconfig /renew” (sem aspas) e aperte **ENTER**. Se um endereço IP válido é mostrado, o acesso à Internet deve estar disponível.
2. Digite “exit” (sem aspas) e aperte **ENTER** para retornar ao Windows.

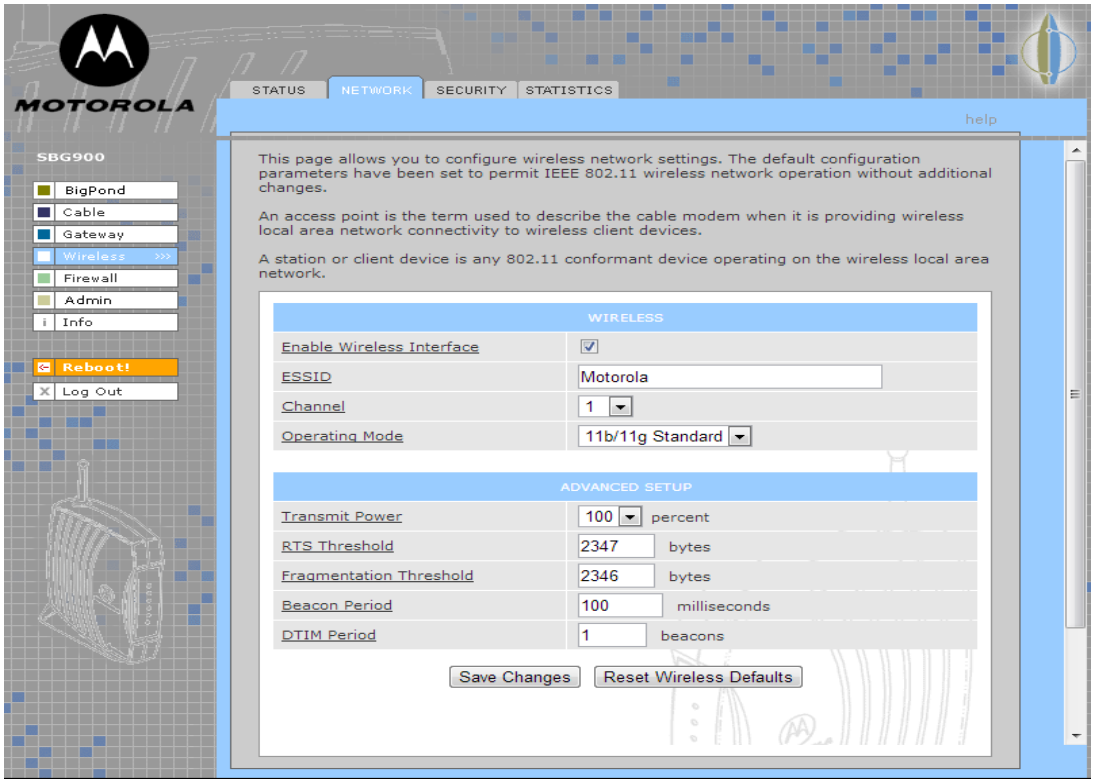
Se depois de realizar esses procedimentos o computador não conseguir acessar a Internet, ligue para seu provedor de serviço a cabo.

❖ Configurando o nome da Rede Sem Fio no SBG900

Se você marcar “Disable ESSID Broadcast” na janela Wireless > Security – Página “advanced”, você deve configurar o mesmo nome de rede (ESSID) em todos os cliente da LAN sem fio. Nunca forneca a ESSID a qualquer um que não está autorizado a usar sua LAN sem fio.

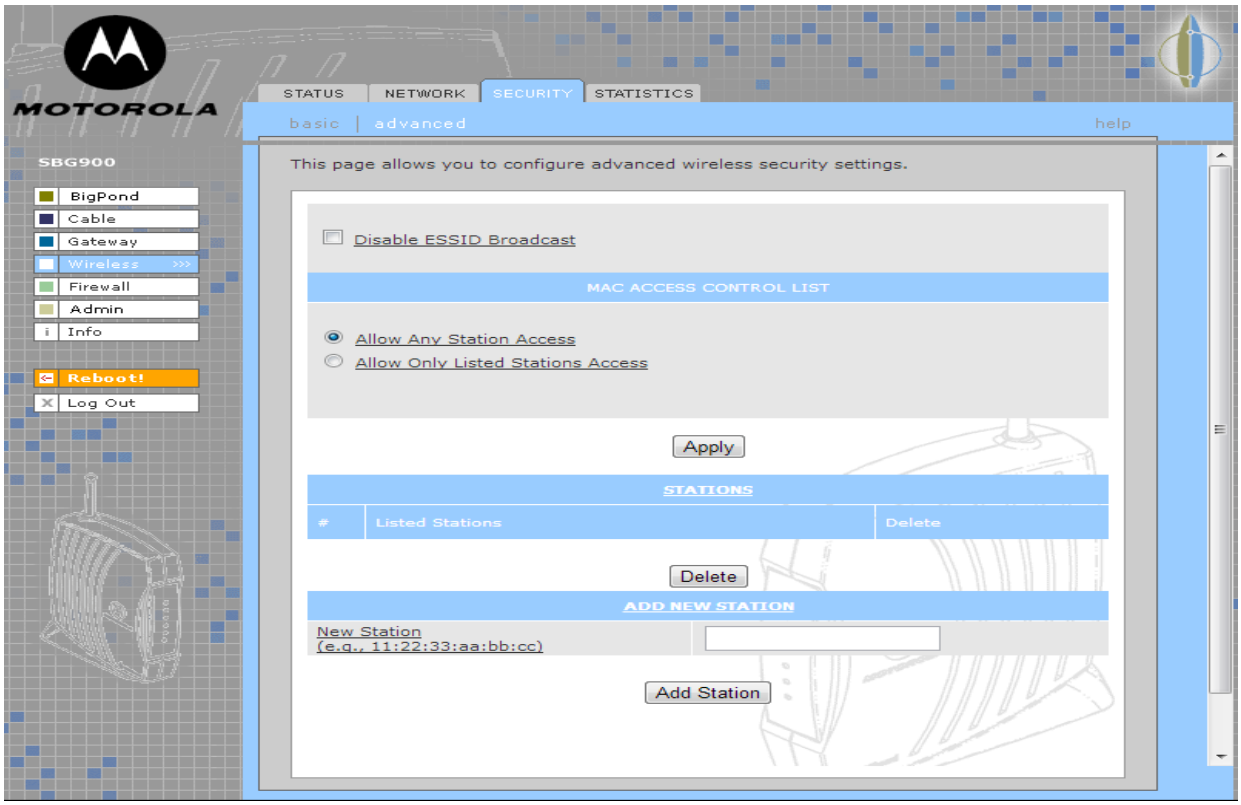
Para configurar ESSID:

1 Inicie o programa de configuração do SBG900.
2 Na aba da esquerda, clique em **Firewall.**
3 Clique na aba **NETWORK** para exibir:



4 No campo **ESSID**, digite um nome único. Pode ser qualquer nome até 32 carácteres alfanuméricos. O padrão é “Motorola” (sem aspas). Não use a ESSID padrão.
5 Clique em **Save Changes** para salvar suas mudanças.
6 Para restringir o acesso à LAN sem fio para clientes configurados com o mesmo Nome de Rede (ESSID) como no SBG900, clique na aba **SECURITY.**

7 Clique em **advanced** para exibir a Wireless > SECURITY – Página “advanced”:



8 Clique em **Disable ESSID Broadcast** para restringir o acesso à LAN sem fio para clientes configurados com o mesmo Nome de Rede (ESSID) que o SBG900.

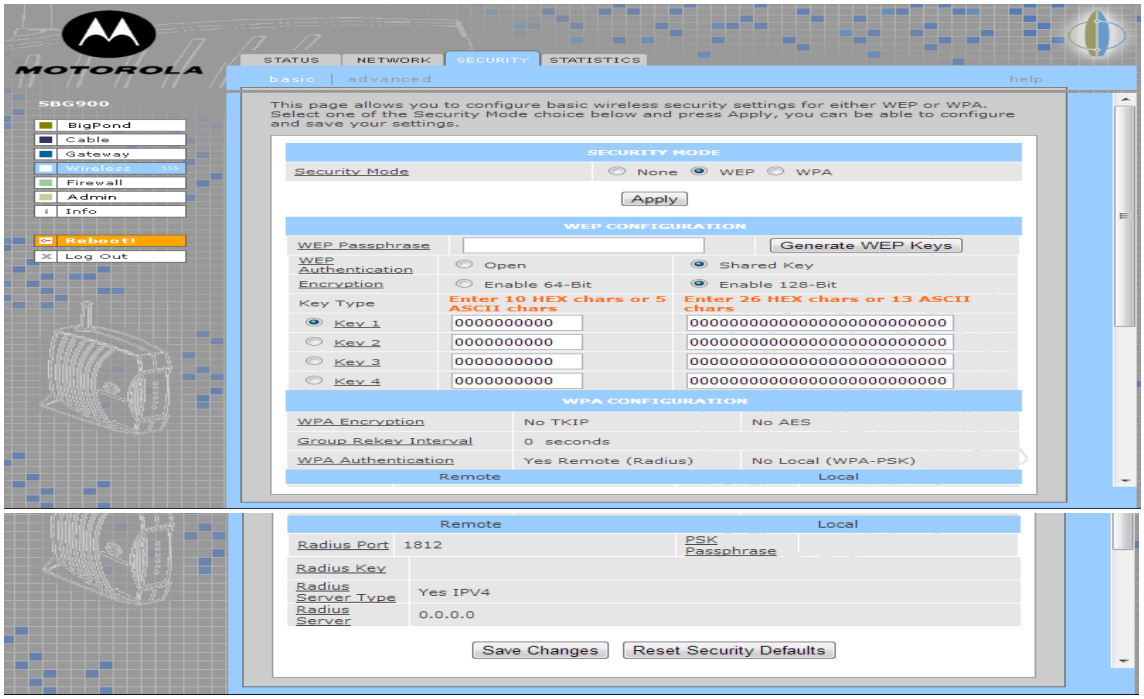
9 Clique em **Apply** para salvar suas mudanças.

❖ Configurando a WEP no SBG900

Para habilitar WEP e definir a chave no SBG900:

1 Na aba esquerda do programa de configuração do SBG900, clique em **Wireless**.

2 Clique na aba **SECURITY** para exibir a **Wireless > SECURITY – Página básica**.



3 Selecione o seguinte:

Authentication Define se a autenticação de chave está ativada para prover privacidade dos dados na LAN sem fio.

Open System – Qualquer cliente da LAN sem fio pode transmitir dados para outro cliente, sem autenticação. Autenticação aberta não provê segurança para dados transmitidos. É o padrão.

Shared Key – Todos os dados transmitidos pela LAN sem fio são encriptados. O SBG900 autentica e transfere dados de/para todos os clientes que tem autenticação de chave compartilhada habilitada e uma chave WEP idêntica.

Encryption Use um tamanho de chave WEP compatível com seus adaptadores de cliente sem fio. Escolha um de:

Enable 64-bit – Use somente se você tiver clientes sem fio que não suportam encriptação 128-bit.

Enable 128-bit – A configuração recomendada para encriptação mais forte; suportada pela maioria dos adaptadores sem fio.

Disable WEP – Recomendado durante a configuração da rede, somente.

Chave 1 a Chave 4 Define a chave WEP ativa. Números de 0 a 9 e carácteres de A a F.

Para encriptação 64-bit, defina uma senha de 10 carácteres.

Para encriptação 128-bit, defina uma senha de 26 carácteres.

4 Clique em **Save Changes** para salvar suas mudanças. Pode ser necessário reiniciar.

❖ Configurando uma Lista de Controle de Acesso por MAC

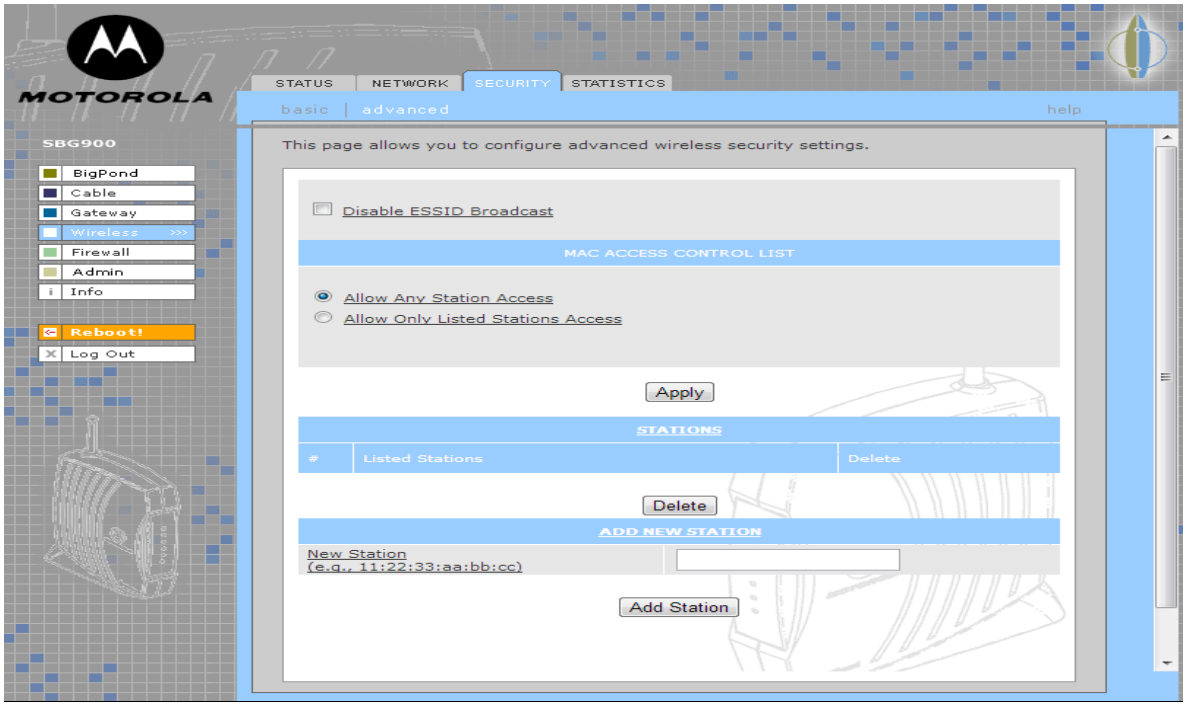
Você pode restringir o acesso sem fio de um a 32 clientes sem fio, baseado no endereço MAC do cliente.

Para configurar a lista de controle de acesso por MAC:

1 Na aba esquerda do programa de configuração do SBG900, clique em Wireless.

2 Clique na aba **SECURITY**.

3 Clique em **advanced** para exibir a **Wireless > SECURITY – Página "advanced":**



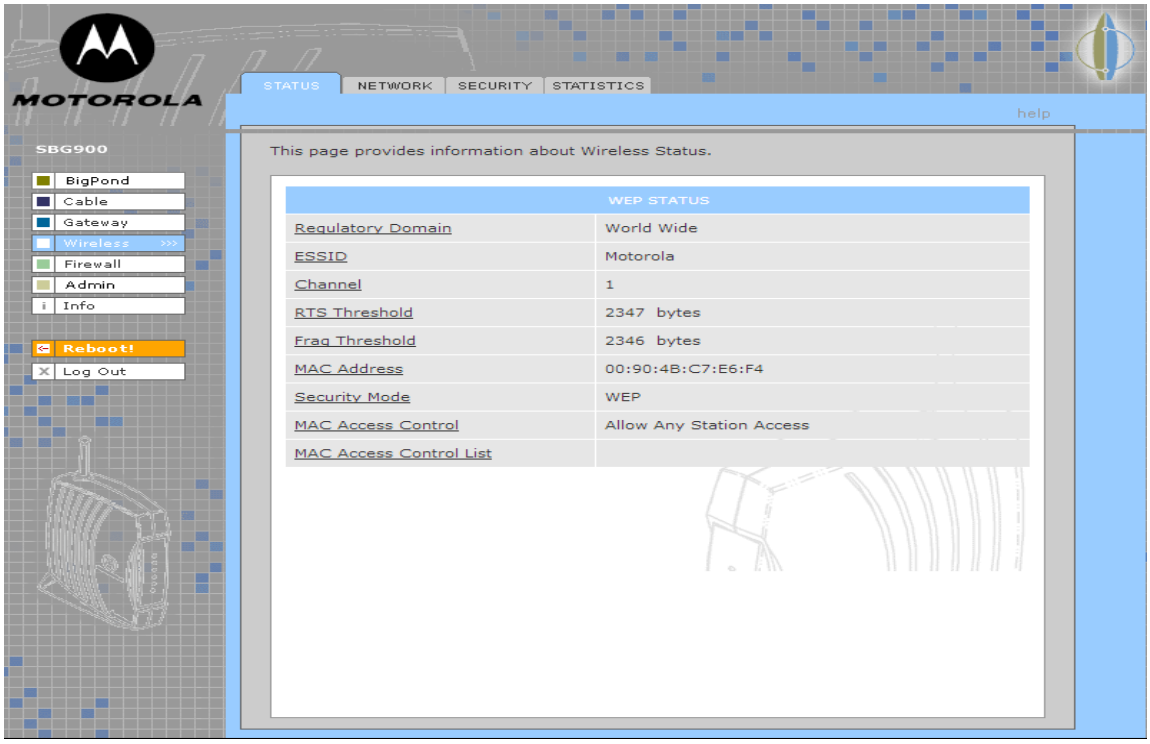
4 Para restringir o acesso sem fio a sistemas na lista de controle de acesso por MAC, marque **Allow Only Listed Stations Access** e clique em **Apply**.

5 Para adicionar um cliente sem fio, digite seu endereço MAC no formato **xx:xx:xx:xx:xx:xx** no campo **New Station** e clique em **Add Station**.

Observação: Você pode adicionar até 32 clientes sem fio à lista de controle de acesso por MAC.

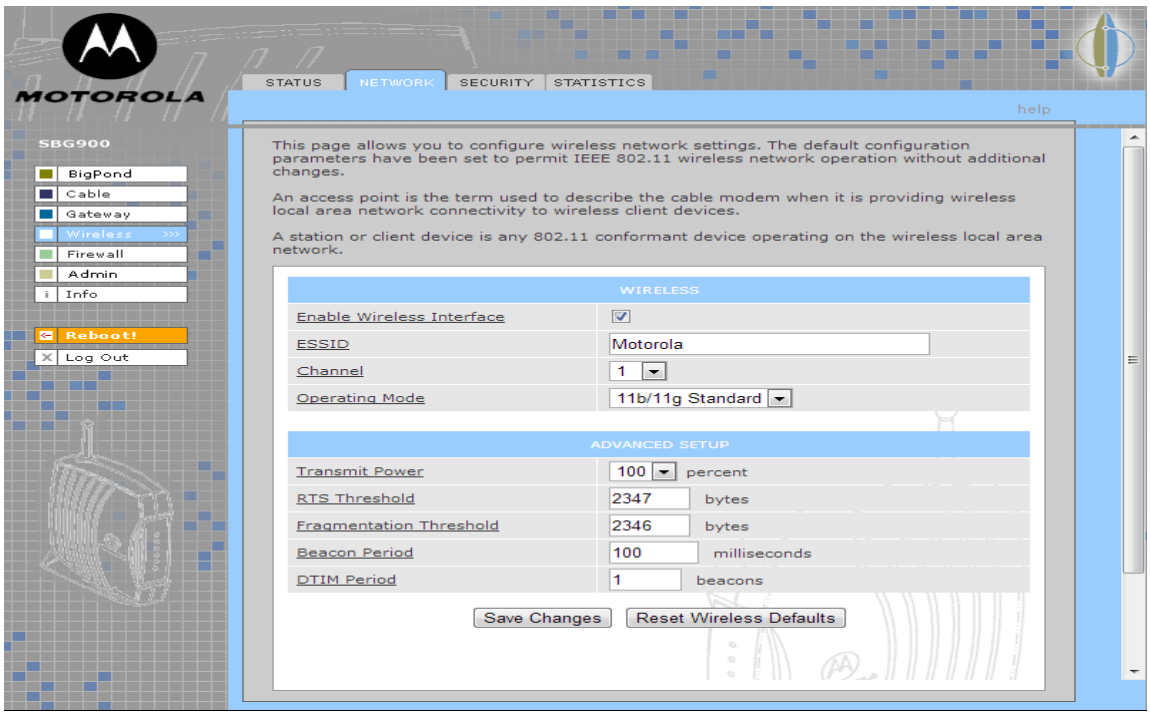
Wireless > Página “STATUS”

Você pode usar esta página para ver o status da interface sem fio.



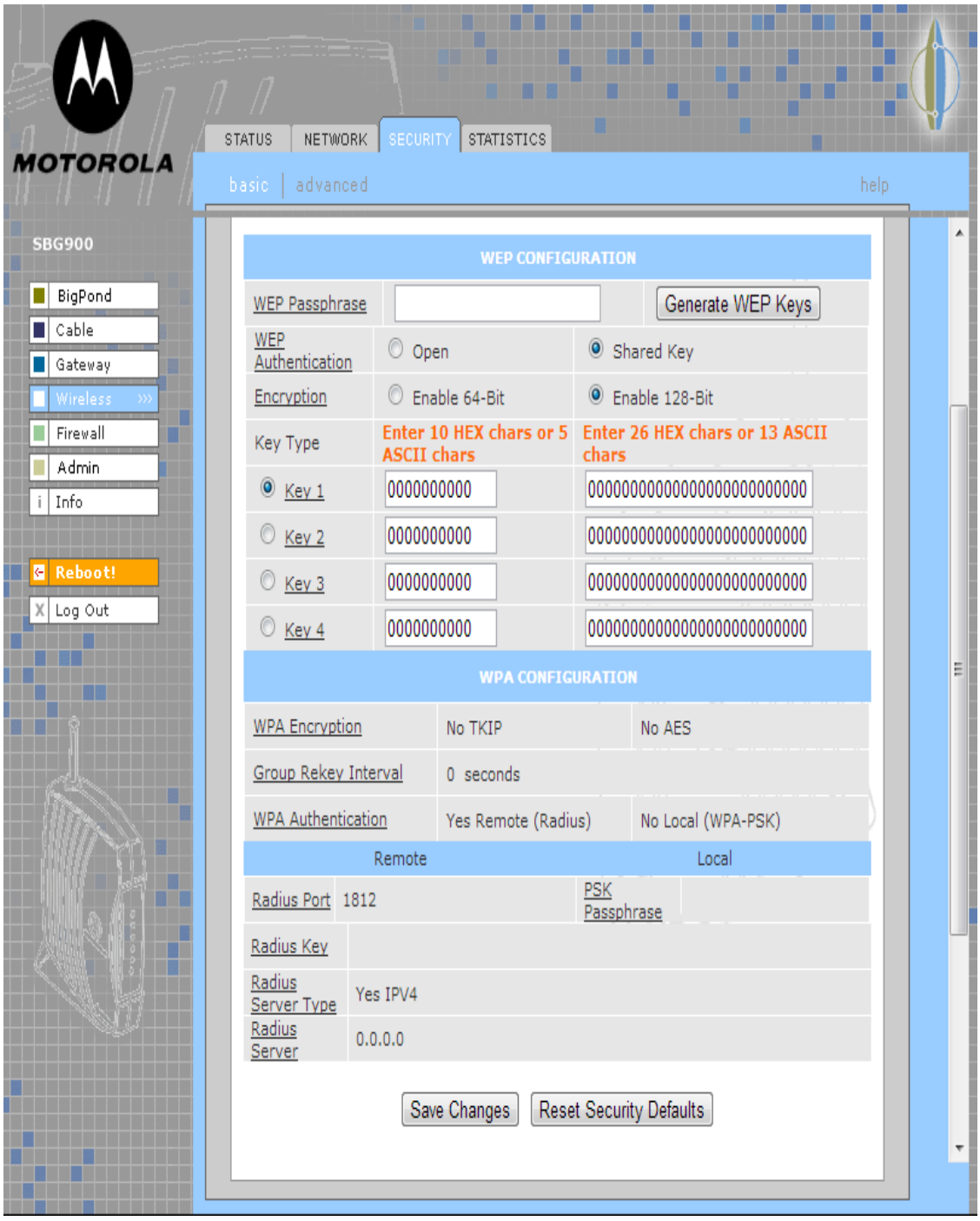
Wireless > Página “NETWORK”

Você pode usar esta página para configurar o nome da rede sem fio e outras configurações da Lan sem fio.



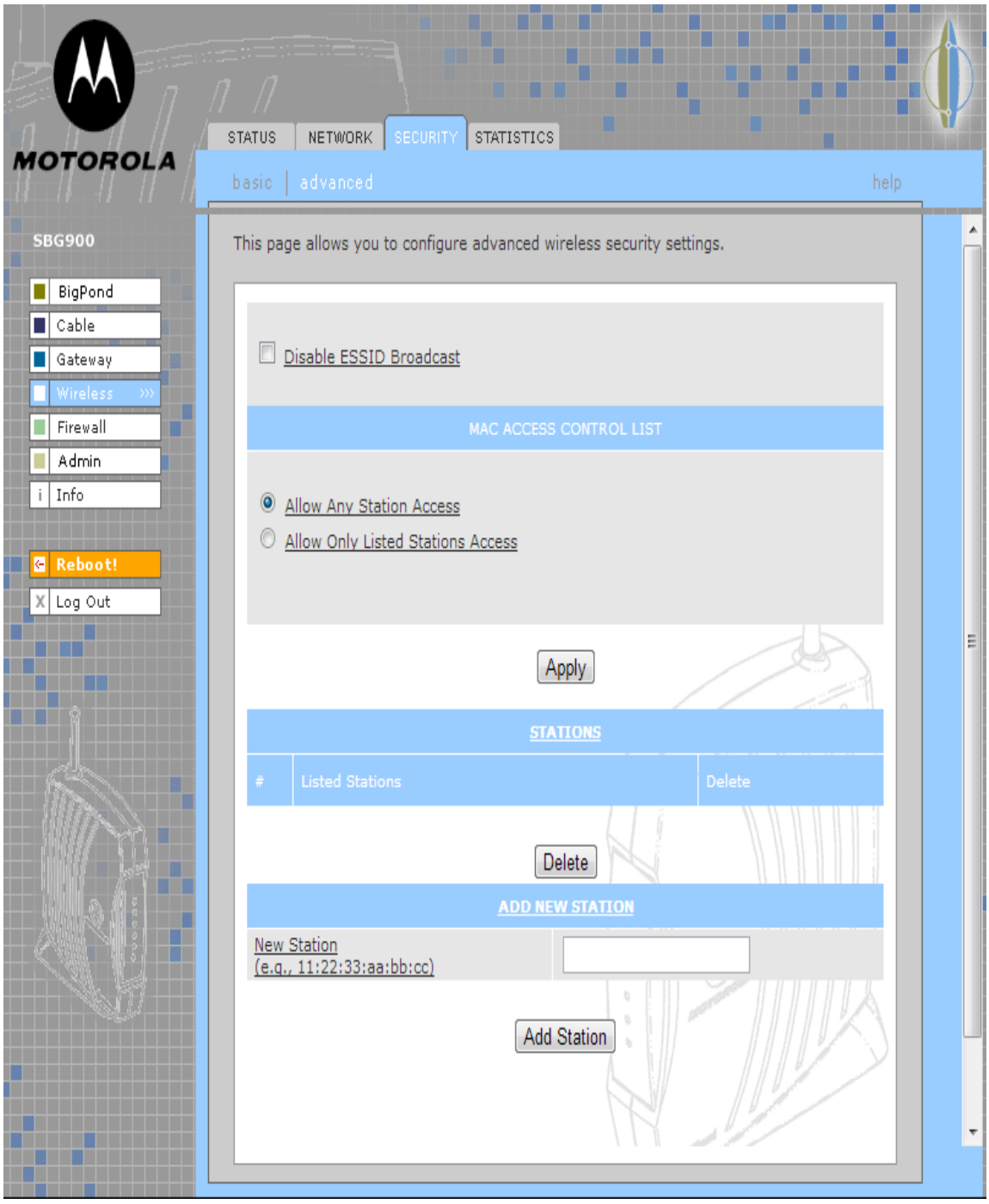
Wireless > SECURITY – Página “basic”

Você pode usar esta página para configurar as configurações da WEP (Pivacidade Equivalente Cabeada).



Wireless > SECURITY – Página “advanced”

Você pode usar esta página para configurar informações avançadas de segurança.



Wireless > Página STATISTICS

Você pode usar esta página para exibir estatísticas da rede sem fio.